

## California Student Data Privacy Addendum

This California Student Data Privacy Addendum (“CA DPA”) is entered into between **Google LLC** (“Google” and/or “Provider”) and **San Joaquin County Office of Education**, with offices at 2922 Transworld Dr, Stockton, California 95206-3952, United States (the “Local Education Agency” and/or “LEA,”), and supplements, amends and is incorporated into the Google Workspace for Education (online) Terms of Service, the Google Cloud Platform (online) Terms of Service, or the Google Cloud Master Agreement (as applicable) between Google and Customer (the “Services Agreement”). Capitalized terms used but not defined in this Addendum have the meaning given to them in the Services Agreement. This CA DPA will be effective as of the last signature date below (the “CA DPA Effective Date”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations

**NOW THEREFORE**, LEA and Provider agree as follows:

**STANDARD CLAUSES**

Version 3.0

**ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of CA DPA.** The purpose of this CA DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. 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. The Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider will process Student Data in accordance with LEA's instructions as described under Google's data processing terms at <https://cloud.google.com/terms/data-processing-addendum>.
  
2. **Student Data to Be Provided.** In order to perform the Services described above, the LEA shall provide Student Data. Student Data is included in the definition of Customer Data as such term is defined in the relevant Service Agreement or Terms of Services. For reference purposes only, the Services Agreement(s) are included below and will only become effective upon their execution. Google terms, in effect as of the Effective Date, state:
  - A. **Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>):
 

*““Customer Data” means data provided to Google by Customer or End Users through the Services under the Account.”*
  
  - B. **Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html)):
 

*““Customer Data” means data submitted, stored, sent or received via the Services by Customer or its End Users.”*
  
3. **CA DPA Definitions.** Definitions used in this CA DPA are found in **Exhibit “C”**. In the event of a conflict, definitions used in this CA DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Privacy Policies etc.

**ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data 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 Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this CA DPA in the same manner as the original Student Data. The parties agree that as between them, all rights, including all intellectual property rights in and to Student Data 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 LEA as it pertains to the use of Student Data, notwithstanding the above.

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

***"5. Intellectual Property Rights; Protection of Customer Data; Feedback.***

**5.1 Intellectual Property Rights.** *Except as expressly stated in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data and Customer Applications, and Google owns all Intellectual Property Rights in the Services and Software.*

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum."*

**B. Google Workspace for Education Services Agreement**  
([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

***"5. Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features Within the Services.***

**5.1 Intellectual Property Rights.** *Except as expressly stated in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.*

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for Advertising purposes or serve Advertising in the Services. Google has implemented and will maintain technical, organizational, and physical, safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum.*

- 2. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider will promptly notify LEA and redirect the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information. If Google's Cloud Data Protection Team receives a request from a parent, legal guardian, or eligible student that relates to Customer Personal Data and identifies Customer, Google will follow the process described in the section Data Subject Requests of the Cloud Data Processing Addendum (as described below).

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the Cloud Data Processing Addendum at <https://cloud.google.com/terms/data-processing-terms>. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum>)

**“9. Access etc.; Data Subject Rights; Data Export**

**9.1 Access; Rectification; Restricted Processing; Portability.** *During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.*

**9.2 Data Subject Requests.**

**9.2.1 Responsibility for Requests.** *During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.*

**9.2.2 Google's Data Subject Request Assistance.** *Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:*

- a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);*
- b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and*
- c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.”*

- 3. Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student- Generated Content to a separate account created by the student.

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. Google will provide the LEA with tools to assist with the above

process. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

*“1.2 Admin Console. Customer will have access to the Admin Console, through which Customer may manage its use of the Services.”*

**B. Google Workspace for Education Services Agreement**  
([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

*“1.2 Admin Console. Customer will have access to the Admin Console, through which Customer may manage its use of the Services.”*

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

Google practices are consistent with LEA’s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

***“7. Confidential Information.***

***7.2 Required Disclosure.*** *Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party’s reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.”*

**B. Google Workspace for Education Services Agreement**  
([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

***“7. Confidential Information.***

***7.2 Required Disclosure.*** *Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its*



*Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual."*

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this CA DPA.

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

A. **Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

*"14.6 Subcontracting. Google may subcontract obligations under the Agreement but will remain liable to Customer for any subcontracted obligations."*

B. **Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

*"15.6 Subcontracting. Google may subcontract obligations under the Agreement but will remain liable to Customer for any subcontracted obligations."*

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from

time to time.

Google practices are consistent with LEA`s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

*“10. **Representations and Warranties.** Each party represents and warrants that (a) it has full power and authority to enter into the Agreement, and (b) it will comply with all laws applicable to its provision, receipt, or use of the Services, as applicable.”*

**B. Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

*“10. **Representations and Warranties.** Each party represents and warrants that (a) it has full power and authority to enter into the Agreement, and (b) it will comply with all laws applicable to its provision, receipt, or use of the Services, as applicable.”*

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this CA DPA.

Google practices are consistent with LEA`s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement, and the Cloud Data Processing Addendum. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

*“5. **Intellectual Property Rights; Protection of Customer Data; Feedback.***

*5.2 **Protection of Customer Data.** Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical, and technical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.”*

**B. Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

*“5. **Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features Within the Services.***

*“5.2 **Protection of Customer Data.** Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for Advertising purposes or serve Advertising in the*

*Services. Google has implemented and will maintain technical, organizational, and physical safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum”*

**C. Cloud Data Processing Addendum (<https://cloud.google.com/terms/data-processing-addendum>)**

***“5.2 Scope of Processing.***

**5.2.1 Compliance with Customer’s Instructions.** *Customer instructs Google to process Customer Data only in accordance the applicable Agreement (including this Addendum) and with applicable law: (a) to provide, secure, and monitor the Services and TSS; and (b) as further specified via (i) Customer’s use of the Services (including the Admin Console and other Services functionality) and TSS; (ii) any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum f (collectively, the “Instructions”). Google will comply with the Instructions unless prohibited by European Law.”*

- 3. Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this CA DPA with respect to the Student 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.

Google practices are consistent with LEA’s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement (<https://cloud.google.com/terms/>)**

***“5. Intellectual Property Rights; Protection of Customer Data; Feedback.***

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical, and technical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.”*

**B. Google Workspace for Education Services Agreement ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))**

***“5. Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features Within the Services.***

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for Advertising purposes or serve Advertising in the*



*Services. Google has implemented and will maintain technical, organizational, and physical safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum.*

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this CA DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this CA DPA. Provider will not Sell Student Data to any third party.

Google practices are consistent with LEA`s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

A. **Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

***“7. Confidential Information.***

***7.2 Required Disclosure.*** *Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.”*

B. **Google Workspace for Education Services Agreement**  
([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

***“7. Confidential Information.***

***7.2 Required Disclosure.*** *Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.”*

5. **De-Identified Data**: Provider agrees not to attempt to re-identify any De-Identified Data. De-Identified Data, may be used by the Provider for those purposes allowed under FERPA and the following purposes:
- (1) assisting the LEA or other governmental agencies in conducting research and other studies; and
  - (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; <sup>1</sup>and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this CA DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de- identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

Google practices are consistent with LEA`s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the Cloud Data Processing Addendum. For reference purposes only, Google terms, in effect as of the Effective Date, state:

A. **Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum>)

**“Appendix 2: Security Measures.**

**Encryption Technologies.** *Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.”*

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within a maximum period of 180 days of the date of said request and according to a schedule and procedure as the parties may reasonably agree. Upon termination of this CA DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3.

Google practices are consistent with LEA`s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the Google Data Processing and Security Terms or the Google Data Processing Amendment, as applicable. For reference purposes only, Google terms, in effect as of the Effective Date, state:

A. **Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum> )

## **“6. Data Deletion**

**6.1 Deletion by Customer.** *Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google’s systems in accordance with applicable law. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.*

**6.2 Return or Deletion When Term Ends.** *If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google’s systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.”*

**6.3 Deferred Deletion Instruction.** *To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Google.”*

- 7. Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this CA DPA and its accompanying exhibits. LEA agrees and acknowledges that the terms of this provision are limited to Google Cloud Platform and Google Workspace for Education services and they do not apply to Additional Products or Third-Party Offerings.

Google practices are consistent with LEA’s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

- A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

## **“5. Intellectual Property Rights; Protection of Customer Data; Feedback.**

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not*

*access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical, measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.”*

**B. Google Workspace for Education Services Agreement**  
([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

**“5. Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features Within the Services.**

**5.2 Protection of Customer Data.** *Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for Advertising purposes or serve Advertising in the Services. Google has implemented and will maintain technical, organizational, and physical safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum.”*

**ARTICLE V: DATA PROVISIONS**

- 1. Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. The LEA must enable the Data Location in the Admin Console.

For clarity, the LEA must enable the Data Location restrictions as a service functionality in the Admin Console. Google further clarifies that any data location restrictions will be subject to the terms of the Cloud Data Processing Addendum. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum>)

**“10. Data Transfers**

**10.1 Data Storage and Processing Facilities.** *Subject to Google’s data location commitments under the Service Specific Terms and to the remainder of this Section 10 (Data Transfers), Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities.”*

- 2. Audits.** Provider will comply with the following terms, unless otherwise specified in the Cloud Data Processing Addendum (<https://cloud.google.com/terms/data-processing-addendum>): :

**A. LEA’s Audit Rights.**

- If European Data Protection Law applies to the processing of Customer Personal Data, Provider will allow LEA or an independent auditor appointed by LEA to conduct audits (including inspections) to verify Provider’s compliance with its obligations under these terms in accordance with Section 2.B (Additional Business Terms for Reviews and Audits) below. During an audit, Provider will make available all information necessary to demonstrate such compliance and contribute to the audit.

- b. If LEA SCCs apply, Provider will allow LEA (or an independent auditor appointed by LEA) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with the Additional Business Terms for Reviews and Audits section.
- c. LEA may conduct an audit to verify Provider's compliance with its obligations under these terms by reviewing Provider's security documentation including compliance certifications and SOC reports (which reflects the outcome of audits conducted by Provider's Third Party Auditor).

**B. Additional Business Terms for Reviews and Audits.**

- a. LEA must send any requests for reviews of the SOC 2 report, or audits, to Provider's Cloud Data Protection Team at <https://support.google.com/cloud/contact/dpo> (and/or via such other means as Provider may provide from time to time).
  - b. Following receipt by Provider of a request, Provider and LEA will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.
  - c. Provider may charge a fee (based on Provider's reasonable costs) for any audit under this Section 2.A. Provider will provide LEA with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. LEA will be responsible for any fees charged by any auditor appointed by LEA to execute any such audit.
  - d. Provider may object in writing to an auditor appointed by LEA to conduct any audit under Section 2.A if the auditor is, in Provider's reasonable opinion, not suitably qualified or independent, a competitor of Provider, or otherwise manifestly unsuitable. Any such objection by Provider will require LEA to appoint another auditor or conduct the audit itself.
3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the cybersecurity framework in **Exhibit "F"**. Provider shall provide contact information of an employee who LEA may contact if there are any data security concerns or questions.

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the Cloud Data Processing Addendum. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum>)

***"Appendix 2: Security Measures***



As from the Terms Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

## 1. Data Center and Network Security

### (a) Data Centers.

*Infrastructure.* Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

*Redundancy.* Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

*Power.* The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

*Server Operating Systems.* Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

*Businesses Continuity.* Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

### (b) Networks and Transmission.

*Data Transmission.* Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

*External Attack Surface.* Google employs multiple layers of network devices and intrusion

*detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.*

*Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:*

- 1. tightly controlling the size and make-up of Google's attack surface through preventative measures;*
- 2. employing intelligent detection controls at data entry points; and*
- 3. employing technologies that automatically remedy certain dangerous situations.*

*Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.*

*Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.*

## *2. Access and Site Controls*

### *(a) Site Controls.*

*On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.*

*Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.*

*On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and*

*the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.*

*(b) Access Control.*

*Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.*

*Access Control and Privilege Management. Customer's administrators and Customer End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.*

*Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.*

*3. Data*

*(a) Data Storage, Isolation and Logging. Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary (e.g., in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data and, for Google Workspace and*



*Cloud Identity: (i) Google logically separates each End User's data from the data of other End Users; and (ii) data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.*

*(b) Decommissioned Disks and Disk Erase Policy. Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.*

#### *4. Personnel Security*

*Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.*

*Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Google's personnel will not process Customer Data without authorization.*

#### *5. Subprocessor Security*

*Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement) of these Addendum, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms."*

- 4. Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider will follow the following process, unless otherwise specified in the Cloud Data Processing Addendum (found at <https://cloud.google.com/terms/data-processing-addendum>) .

- A. *Incident Notification. Provider will notify LEA promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure*

Customer Data.

- B. Details of Data Incident. Provider's notification of a Data Incident will describe: the nature of the Data Incident including the LEA resources impacted; the measures Provider has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Provider recommends that LEA take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Provider's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.
- C. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address.
- D. No Assessment of Customer Data by Provider. Provider has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.
- E. No Acknowledgement of Fault by Provider. Provider's notification of or response to a Data Incident under this provision, will not be construed as an acknowledgement by Provider of any fault or liability with respect to the Data Incident.

**ARTICLE VI: GENERAL OFFER OF TERMS  
RESERVED**

**ARTICLE VII: MISCELLANEOUS**

1. **Termination.** In the event that either party seeks to terminate this CA DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this CA DPA and any service agreement or contract if the other party breaches any terms of this CA DPA.

Google practices are consistent with LEA's requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement. For reference purposes only, Google terms, in effect as of the Effective Date, state:

- A. **Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

**"8. Term and Termination.**

**8.2 Termination for Breach.** To the extent permitted by applicable law, either party may terminate this Agreement immediately on written notice if (a) the other party is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice of the breach or (b) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within 90 days."

- B. **Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))



**“8. Term and Termination.**

**8.3 Termination for Breach.** *To the extent permitted by applicable law, either party may terminate this Agreement immediately on written notice if (a) the other party is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written notice of the breach, or (b) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within 90 days.”*

2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA’s Student Data pursuant to Article IV, section 6.

Google practices are consistent with LEA’s requirements specified in the provision above. Google further clarifies that it will comply with this provision in accordance with the terms described in the relevant Services Agreement, and the Cloud Data Processing Addendum. For reference purposes only, Google terms, in effect as of the Effective Date, state:

**A. Google Cloud Platform Services Agreement** (<https://cloud.google.com/terms/>)

**“8. Term and Termination.**

**8.6 Effect of Termination.** *If the Agreement is terminated, then (a) all rights and access to the Services will terminate (including access to Customer Data, if applicable), unless otherwise described in this Agreement, and (b) all Fees owed by Customer to Google are immediately due upon Customer’s receipt of the final electronic bill or as stated in the final invoice.”*

**B. Google Workspace for Education Services Agreement** ([https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html))

**“8. Term and Termination.**

**8.6 Effect of Termination or Non-Renewal.** *If the Agreement is terminated or not renewed, then (a) all rights and access to the Services will cease (including access to Customer Data), unless otherwise described in this Agreement, and (b) any and all Fees owed by Customer to Google are immediately due upon Customer’s receipt of the final invoice.”*

**C. Cloud Data Processing Addendum** (<https://cloud.google.com/terms/data-processing-addendum>)

**“6. Data Deletion**

**6.2 Return or Deletion When Term Ends.** *If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google’s systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.”*

3. **Priority of Agreements.** This CA DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this CA DPA. In the event there is conflict between the terms of the CA DPA and the Service Agreement (the Service Agreement includes: Google Terms of Service, Google Privacy Policies, any other bid/RFP, Google license agreement or writing, the terms of the Service Agreement (including the Cloud Data Processing Addendum)), the Services Agreement shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This CA DPA and the relevant Service Agreement (including the URL Terms (as such term is defined in the relevant Services Agreement)) constitute 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 CA DPA may be amended and the observance of any provision of this CA 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.
5. **Severability.** Any provision of this CA 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 CA 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 CA DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS CA DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE FOLLOWING:
  - (a) For U.S. City, County, and State Government Entities. If Customer is a U.S. city, county, or state government entity, then the Services Agreement will be silent regarding governing law and venue.
  - (b) For U.S. Federal Government Entities. If Customer is a U.S. federal government entity, then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THE SERVICES AGREEMENT OR THE SERVICES WILL BE GOVERNED BY THE LAWS OF THE UNITED STATES OF AMERICA, EXCLUDING ITS CONFLICT OF LAWS RULES. SOLELY TO THE EXTENT PERMITTED BY FEDERAL LAW, (I) THE LAWS OF THE STATE OF CALIFORNIA (EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES) WILL APPLY IN THE ABSENCE OF APPLICABLE FEDERAL LAW; AND (II) FOR ALL CLAIMS ARISING OUT OF OR RELATING TO THE SERVICES AGREEMENT OR THE SERVICES, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

(c) For All Other Entities. If Customer is any entity not identified in Section 14.12(a) (U.S. Governing Law for U.S. City, County, and State Government Entities) or (b) (U.S. Governing Law for Federal Government Entities), then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THE SERVICES AGREEMENT OR THE SERVICES WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING THAT STATE'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

**7. Successors Bound:**

**A. Assignment.** Neither party may assign any part of this CA DPA without the written consent of the other, except to an Affiliate where (a) the assignee has agreed in writing to be bound by the terms of this CA DPA, and (b) the assigning party has notified the other party of the assignment. Any other attempt to assign is void. If LEA assigns this CA DPA to an Affiliate in another jurisdiction such that there is a change in the Provider contracting entity as defined at <https://cloud.google.com/terms/google-entity> (i) this CA DPA is automatically assigned to the new Provider contracting entity.

**B. Change of Control.** If a party experiences a change of Control other than as part of an internal restructuring or reorganization (for example, through a stock purchase or sale, merger, or other form of corporate transaction), that party will give written notice to the other party within 30 days after the change of control.

**8. Authority.** Each party represents that it is authorized to bind to the terms of this CA DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

**9. Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**10. Conflicting Terms.** In the event there is conflict between the terms of the CA DPA and any other writing, including, but not limited to the Service Agreement, the terms of the Services Agreement shall control.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT (RESOURCE) HERE]

Google Cloud services are listed in the Google Cloud Platform Services Summary at <https://cloud.google.com/terms/services> including but not limited to App Engine, Compute Engine, Google Cloud VMware Engine (GCVE), Cloud Storage, BigQuery, among others

Google Workspace for Education Services are listed in the Google Workspace Services Summary at [https://workspace.google.com/intl/en/terms/user\\_features.html](https://workspace.google.com/intl/en/terms/user_features.html) including but not limited to Google Workspace for Education Fundamentals, Google Workspace for Education Standard, Google Workspace for Education Teaching and Learning Upgrade, and Google Workspace for Education Plus.

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Google processes Customer Data in order to provide its Cloud Services and in accordance with Customer's Instructions and applicable law. The LEAs have full and total control over which data elements are submitted to Google and shall have full access to all data it submits to Google. The LEA shall have full control over which users it authorizes at all times. Customer Data is encrypted at rest and in transit as described at the following links <https://cloud.google.com/docs/security/encryption/default-encryption> and <https://cloud.google.com/docs/security/encryption-in-transit>

**EXHIBIT “C”**  
**DEFINITIONS**

**Additional Products** means products, services and applications that are not part of the Services but that may be accessible for use in conjunction with the Services.

**Confidential Information:** Information that one party or its Affiliate (“Disclosing Party”) discloses to the other party (“Recipient”) under the Services Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. Customer Data is Customer’s Confidential Information. Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.

**Controller** has the meaning given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies. LEA is a controller or processor, as applicable, of Customer Personal Data.

**Customer Data:** For Google Cloud Platform Customer Data means data provided to Google by Customer or End Users through the Services under the Account. For Google Workspace for Education Services Customer Data means data submitted, stored, sent or received via the Services by Customer or its End Users. For clarity purposes, Student Data is included in the definition of Customer Data.

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For sake of clarity, Education Records is “Customer Data” as such term is defined in the relevant Services Agreement found at: (a) for GCP, <https://cloud.google.com/terms/>; and (b) for Google Workspace for Education, [https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html)

**LEA or Local Education Agency** means K12 school districts including public, private and charter schools. LEA excludes higher education schools and/or universities.

**Originating LEA** means a LEA who originally executes the CA DPA in its entirety with the Provider.

**Processor** has the meaning given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies. LEA is a controller or processor, as applicable, of Customer



Personal Data. Google is a processor of Customer Personal Data.

**Provider** means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data, or otherwise defined in applicable regulation or law.

**Student Generated Content** means materials or content created by a student in the services 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 student content. For sake of clarity, Student Generated Content is “Customer Data” as such term is defined in the relevant Services Agreement found at: (a) for GCP, <https://cloud.google.com/terms/>; and (b) for Google Workspace for Education, [https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html).

**School Official:** For the purposes of this CA DPA and pursuant to 34 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re- disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Provider’s contract, purchase order or terms of service or terms of use including but not limited to the Google Workspace for Education (online) Terms of Service, the Google Cloud Platform (online) Terms of Service, and/or the Google Cloud Master Agreement (as applicable) between Google and Customer.

**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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents’ names, or any other information or identification number that would provide information about a specific student. Student Data may include personal identifiable information that is maintained and/or stored by Provider. Student Data further includes “personally identifiable information (PII),” as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this CA DPA, and for the purposes of federal, state, and local laws and regulations. Student Data shall not constitute information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services. For sake of clarity, Student Data is “Customer Data” as such term is defined in the relevant Services Agreement found at: (a) for GCP, <https://cloud.google.com/terms/>; (b) for Google Workspace for Education, [https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html); and/or (c) the Google Cloud Master Agreement.

**Subprocessor:** For the purposes of this CA DPA, 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 service, and who has access to Student

Data.

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

**Targeted Advertising** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third-Party Offerings** means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software and/or (b) offerings identified in the third-party terms section of the relevant service specific terms.

**EXHIBIT "D"**  
**RESERVED**



**EXHIBIT "E"**  
**RESERVED**



**EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

Google products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. Google Cloud certifications and the compliance standards information can be found at <https://cloud.google.com/security/compliance/>

The security measures undertaken by Provider pursuant to this CA DPA are described in Article V of the main text. Further descriptions of the security measure employed by Provider may be found at the following link:

- Cloud Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum>

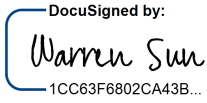
**EXHIBIT "G"**  
**RESERVED**

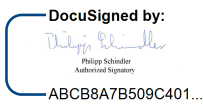


**IN WITNESS WHEREOF**, LEA and Provider execute this Amendment as of the Effective Date.

LEA: **San Joaquin County Office of Education**

Provider: **Google LLC**

By: 

By: 

Print Name:

Print Name:

Title:

Title:

Date:

Date:

