Fagen Friedman & Fulfrost LLP

70 Washington Street, Suite 205
Oakland, California 94607
Main: 510-550-8200
Fax: 510-550-8211
www.f3law.com

Mark S. Williams
Direct Dial: 510-550-8228
mwilliams@f3law.com

October 6, 2016

VIA ELECTRONIC MAIL
andrea.bennett@cetpa.net

Ms. Andrea Bennett
Chief Executive Officer
CETPA
980 9th Street, 11th Floor, Suite 21
Sacramento, CA 95814

Re: Compliance of Google G Suite for Education with FERPA and AB 1584

Dear Ms. Bennett:

We have undertaken the task of determining whether the Google Apps For Education ("GAFE"), recently renamed G Suite for Education ("G Suite"), complies with Federal and State of California student privacy laws. As you know, G Suite is a suite of digital products that Google states is "productivity tools for classroom collaboration." G Suite products are in wide use, both in California school districts and elsewhere. School districts will be referred to as local educational agencies ("LEA") for this discussion. One study from 2015 estimated that over 40 million users used G Suite products in the classroom worldwide and that number is expected to exceed 110 million users by the year 2020.[1] It appears that these global numbers will be met. Google confirmed recently that G Suite users have recently reached 60 million, with 30,000 Chromebooks being activated each day.

Executive Summary: We have concluded that G Suite complies with Family Educational Rights and Privacy Act ("FERPA") and California Education Code section 49073.1 (commonly referred to by its legislative enactment, "AB 1584"). Our conclusions rests on several factors. Notably, the G Suite Agreement is not a single document, but actually consists of a set of several documents. These documents include enforceable instruments, as well as authoritative reference documents that can be used to interpret the G Suite Agreement. Taken together, this multi-document G Suite Agreement explicitly satisfies most required elements of AB 1584 and FERPA.

The only requirement set forth in AB 1584, that is not found directly in the G Suite Agreement, is the opportunity for parents or students to review and correct erroneous student records. This

[1] PRNewswire, July 1, 2015

omission is not fatal to the Agreement. We do not believe these statutes intended to require a direct procedural and technical relationship between Google and the parent or student on this subject. In our view, any substantive decision to modify or delete student records is reserved, and must be reserved, exclusively for the relationship between the LEA and the parent or student. Google's role is to maintain the technical capability and contractual willingness to implement the LEAs directives.

We think this finding regarding the opportunity for review and correction of student records is important, not only for an examination of G Suite products, but as a methodology to determine compliance with other digital educational products. Many other education apps might otherwise fail to meet the AB 1584 "checklist", if not examined in this way.

Our findings are consistent with the conclusions reached by Ernst & Young's audit of Google Products, including G Suite, for data privacy and security. Ernst & Young audited Google's compliance with International Standards Organization ("ISO") criteria. The ISO criteria is different in some ways from AB 1584 and FERPA, but also overlaps in important ways. The issuance by Ernst and Young of Certificates of Compliance for G Suite for both the data security and data privacy standards of ISO is a powerful verification of our findings.

It should be noted that our findings pertain to "Core" G Suite products only (e.g. Gmail, Calendar, Classroom, Sheets, Drive, Docs, Vault and Groups). This point should be emphasized because many educators have recently begun using Google products that Google lists in G Suite materials as "Additional Services." In many cases, these "Additional Services" do not have the same range of privacy guarantees as G Suite "core" products and sometimes require parental consent before the LEA can use them.

This confusion can be abated by a simple observation. The products identified as G Suite "Additional Services" are in fact products for a different Google product line, "Google Apps for Work." Applications for the business world would obviously not be designed to comply with FERPA or AB 1584. How the LEA would administratively and legally manage a migration to these business-based product lines will be the basis of a subsequent writing.

It should be noted that our conclusion that G Suite is student privacy compliant is based on a review of the contract documents, certifications, and accounting standards attached to this letter. Our opinion does not encompass previous versions of these documents, nor will it apply to future G Suite contracts in the event they are materially modified.

1. Introduction and Applicable Statutes

The original and primary Federal statute establishing requirements for student records and privacy is FERPA (found at Title 20, section 1232 (g), et seq.). The primary California student privacy law is recently enacted AB 1584. FERPA requires the LEA to insure that student records are kept confidential unless they are used or disclosed according to enumerated exceptions. AB 1584 requires that contracts between the LEA and digital storage and educational software companies ("Digital Providers") contain affirmative provisions insuring certain privacy protections. FERPA and AB 1584 requirements are mostly "intertwined" because AB 1584 expressly incorporates FERPA as a contract provision. (California Education Code section 49073.1 (b) (8)).

The LEA that does not comply with FERPA potentially subjects itself to action by the United States Department of Education, which can theoretically terminate Federal education funding. A violation of AB 1584 renders "void" any contracts between the LEA and the Digital Provider. (California Education Code section 49073.1 (c)).

In addition to FERPA and AB 1584, our review will also include California Civil Code section 1798.82. This statute requires businesses that store personal information to take specific actions and provide defined notices to individuals in the event of an unauthorized access to "personal information." Although section 1798.82 is a "stand-alone" statutory requirement, it is also the most logical way a Data Provider can comply with section 49073.1 (b) of AB 1584. This subsection requires a "description of the procedures for notifying the affected parent, legal guardian or eligible pupil in the event of an unauthorized disclosure of the pupil's records."

Surprisingly, despite the widespread use of G Suite and the importance of the LEA's legal compliance with privacy laws, we were unable to find any analysis of whether G Suite actually complies with either FERPA or AB 1584. Some writings simply state that since G Suite operates in a subject matter governed by FERPA, G Suite must therefore comply with FERPA. We think the LEA's deserve something more than a conclusion and therefore this analysis is needed.

2. Previous Certifications and Audits

Introduction: Although there has been little legal literature assessing Google's compliance with FERPA and California education law, a great deal of study has been undertaken to determine G Suite's compliance with other standards for data security and privacy. These standards are ISO 27001, ISO 27018, and SOC 2. Specifically, three audits of G Suite Products were undertaken by Ernst & Young to determine whether G Suite complied with these standards. (The studies referred to the Google products under their former name of "GAFE", they are referred to below as "G Suite" to avoid confusion.) Ernst & Young concluded that G Suite met these standards and issued Certificates of Compliance.

It is difficult to overstate the importance of these findings. First, the audits show an adherence of G Suite documents and policies to privacy and security standards (essentially the same exercise we are undertaking in this letter). Second, the audit went beyond a review of contract documents and examined Google practices, that is, whether Google acted in a manner consistent with its agreements and policies. Third, the standards in most respects are more demanding and detailed than those found in AB 1584. Finally, and perhaps most importantly, the lengthy standards set forth in ISO 27001 and 27018 are expressly incorporated into the G Suite Agreement (See Article 6.4 of the Data Processing Amendment). It is a fair presumption that these standards are "gap fillers" for any incompleteness or ambiguity in the other G Suite Agreement documents.

We will set out first the review of international compliance and then with G Suite compliance within the United States.

(a) ISO Standard 27001: The international standards examined by Ernst & Young have been set by a group called the International Standards Organization ("ISO"), an international organization that sets authoritative standards and best practices in a wide variety of economic, professional and business activities. One such standard is the ISO 27001 Certification, which addresses computer processors adherence to data security. Organizations obtaining a Certification have satisfied 114 "controls" or objectives addressing data security. Ernst & Young conducted an audit of Google Products, including G Suite, and issued a 27001 Certificate in 2012. It was renewed in 2015 and is considered effective through 2018. (Copies of the ISO/IEC Security Certificates are attached hereto as **Exhibit "A"**). This Certificate attests that Google has met international standards for data security. Since our subsequent analysis shows Google undertaking security measures in a comprehensive manner, we will not detail the audit standards and findings here.

(b) ISO Standard 27018: ISO also created ISO/IEC 27018:2014 ("ISO 27018"), which establishes a standard that includes data privacy and security for personally identifiable information ("PII"). ISO 27018 contains a number of standards closely related to those set forth in AB 1584 and Civil Code section 1789.25. (This is particularly true for the Annex to ISO 27018). Ernst & Young also issued an ISO 27018 Certificate to Google. (This Certificate is attached hereto as **Exhibit "B"**). Only a few sections of ISO 27018 will be analyzed in detail here. (Some will be referenced later, in our analysis of AB 1584).

(i) No Advertising: In order to receive a Certificate, Processors (processors are vendors like Google), must agree not to utilize the data provided to it for marketing or advertising. (A.2.2) Interestingly, this requirement flows out of an earlier requirement that the data received should not be used for any unauthorized purpose. (A.2.1) As we shall see below, a prohibition against unauthorized use and advertising are explicit requirements of AB 1584 (Education Code sections 49073.1 (b) (3) and (9).)

(ii) Data Retention and Disposal: ISO 27018 requires a wide variety of specific security practices to maintain the security of stored data and to ensure their return when contractual services are completed. For example, section A.4.1 requires that temporary files and documents should be erased within a specified documented period, presumably so that copies of documents do not multiply, undermining effective tracking and control. Section A.4.1 is one of several controls and guidance found in ISO 27018 that relates to the disposal of data, both during the life of a contractual relationship between Google and a Customer and after the ending of that contractual relationship.

These sections include A.9.3 (return, transfer and disposal of data), and A.10.2 (restriction of hard copies of data). These sections address the same subject matter of AB 1584, requiring the return of data after the conclusion of the contract. It is apparent that the ISO 27018 has more sweeping and detailed data return and destruction standards than those found in AB 1584. (Although it might be instructive to quote these and other sections here, they would be digressive for our purposes and unduly reveal IOS 27018 language, which is protected by copyright).

(iii) Notification of Data Breach

Pursuant to section 9.1, a public cloud data processor like Google should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII. The Annex contains a number of sections regulating in some detail a Processor's duties in the event of unauthorized access to PII, as required by AB 1584. The specific steps taken match almost exactly the substantive requirements California Civil Code section 1789.25. These include a description of the incident, a description of the data compromised, the name of the reporter to whom the incident was reported, and the steps taken to resolve the incident.

(c) SOC Type II and SOC 3 Audits.

A Service Organization Control report has a predefined set of principles and related criteria that are defined by the American Institute of Certified Public Accountants ("AICPA") and must be met to achieve an unqualified report. The criteria for SOC 2 are widely recognized. The SOC 3 Report asserts publicly that G Suite are in conformity with the AICPA for security, availability, process integrity and confidentiality. (A copy of the Report is attached hereto as **Exhibit "C"**). The Report summarized its findings as follows:

"Google Inc.(the Company) maintained effective controls over the security, availability, processing integrity and confidentiality of its Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and other Google Services (System) to provide reasonable assurances that:

- the System was protected against unauthorized access, use or modification;
- the System was available for operation and use as committed and agreed;
- the System processing was completely accurate, timely and authorized; and
- the System information designated as confidential was protect as committed or agreed."

3. Methodology of FERPA and AB 1584 Review

It may be helpful to set out the assumptions and limitations of our review so that our conclusions can be viewed with clarity. We set them out below:

(a) Document Review and not an Audit

Our review of whether G Suite products complies with FERPA and AB 1584 is restricted to a review of the G Suite Agreement and associated documents. Unlike Ernst & Young, we did not conduct an audit to determine whether Google adheres to the privacy requirements of FERPA and AB 1584 in practice. (As we have seen above the Ernst & Young audits and Certificates should provide concerned educators with reasonable assurance on this topic).

(b) The G Suite Agreement is a Collection of Documents

In order to perform a complete analysis of G Suite compliance, our analysis will include more than an examination of the G Suite for Education Online Agreement ("G Suite Online Agreement") by itself. Our review will also include other documents which are referenced or incorporated into the G Suite Agreement, or can otherwise explain the G Suite Agreement terms. Google has set forth the following documents as being components of the G Suite Agreement:

1. G-Suite for Education Online Agreement. (**Exhibit "D"**)

2. G Suite for Education Privacy Notice. (**Exhibit "E"**)

3. Additional Terms For Use of Additional Services. (**Exhibit "F"**)

4. Data Processing Amendment to G-Suite Online Agreement. (Sometimes referred to as "DPA" and attached hereto as **Exhibit "G"**)

There are additional documents which also supplement or provide other explanatory material to interpret the four documents referred to above. These include:

5. Google for Education: Tools School can Trust. (**Exhibit "H"**)

6. Privacy Policy (Referred to in the Privacy Notice) (**Exhibit "I"**)

7. Google for Security and Compliance Whitepaper ("Whitepaper") (**Exhibit "J"**)

8. ISO 27001 (Not attached for reasons of copyright)

9. ISO 27018 (Not attached for reasons of copyright)

10. SOC 2 Report (Already attached, as **Exhibit "C"**)

Under California law an agreement can consist of several documents, so long as the parties intend them to be of the same transaction. Indeed purchases of property and construction agreements frequently consist of separately prepared documents and agreements, all related to the same transaction. This understanding is crucial to our review. By itself, the G Suite Online Agreement does not appear to contain all required terms, so that an educator or legal practitioner reviewing the document alone could reasonably conclude that G Suite does not comply with FERPA or AB 1584. However, when read together, the documents point to a different conclusion.[2]

(c) The Challenges of Word Usage

[2] Pursuant to California Civil Code section 1642, several contracts relating to the same matter and made as parts of the same transaction are to be taken together. (See also Witkin, *Summary of California Law*, Volume 1, Contracts, section 1642).

Perhaps the greatest challenge in reviewing the G Suite Agreement is word usage. FERPA and AB 1584 use certain defined terms and phrases to describe particular subjects or issues, while the G Suite Agreement often employs words and phrases that are similar but perhaps convey subtly different meanings. The occasional differences in phrasing between the applicable statutes and the G Suite Agreement may have something to do with the scope of the G Suite Agreement. The G Suite Agreement is a global document and crafted to satisfy a multiplicity of statutes and treaties. Google is naturally reluctant to modify this language to satisfy the requirements of a particular jurisdiction. Although understandable, this variance in terms complicates our task.

Where there is a variance in terms, we will first determine if the word in question is a synonym or an equivalent. If this effort is not successful we will then determine, whether the alternative phrasing describes a right or process that meets the function or objective of the underlying statute.

4. AB 1584 and FERPA Review

As we have stated above, AB 1584 applies to the LEAs when entering into contracts with third-parties who will:

"(1) Provide services, including cloud-based services, for the digital storage, and management and retrieval of pupil records; or

(2) Provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records…" (California Education Code section 49073.1(a).

G Suite performs both statutory functions. Therefore, the G Suite Agreement must address nine requirements set forth in the statute. We set them out below and analyze each issue. As we move through our analysis of AB 1584, we will note, where appropriate, the analogous FERPA requirement. In some cases there will not be a direct FERPA analog, such as cases of data breach notification. (It could be argued nonetheless that the additional requirements of AB 1584 fully realize the purposes and implications of FERPA).

1. <u>Does the G Suite Agreement Provide a Statement that Pupil Records Continue to be the Property of and under the Control of the LEA? (California Education Code section 49073.1(b)(1)</u>

This section is a perfect example of differences in word choice. The G Suite Agreement recognizes that the Pupil Records "continues to be the property of and under the control of the district". This is a perfect illustration of the value of understanding synonymous language and the need to read each component of the G Suite Online Agreement "Pupil Records" are defined elsewhere in California Education Code section 49073.1 as:

(i) Any information directly related to a pupil that is maintained by the local educational agency.

(ii) 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 agency employee.

The G Suite Agreement does not explicitly use the term "Pupil Records". However it does use the term "Customer Data", which as defined, would subsume the set of data called "Pupil Records." "Customer Data" is defined in the G Suite Agreement as all data provided, generated, transmitted or displayed by Customer or End Users (G Suite Online Agreement, section 16; DPA, section 2). Google then confirms that Customer Data explicitly includes "personally identifiable information from records that are subject to FERPA." (G Suite Online Agreement, section 7.4). Google therefore explicitly satisfies FERPA as to the types of data that will be given protection by the G Suite Agreement.

This result is confirmed by looking at examples of the types of data listed by the G Suite Online Agreement as protected. Appendix 1 to the DPA provides wide ranging examples of data to include "User Ids, emails, documents, presentations, images calendar entries, tasks and other electronic data". These illustrations of Customer Data are equivalent to the examples of "pupil-generated content" found at 49073.1 (d)(4):

"[E]ssays, research reports, portfolios, creative writing, music or other audio files, photographs and account information that enables ongoing ownership of pupil content."

Having established that "Customer Data" and "Pupil Records" are equivalent terms we must then determine whether the G Suite Agreement satisfies the requirement that the data "remains the property and under the control of the District". The DPA explicitly satisfies the "control" element of the standard when it states, at Article 5.1: "Customer is the Controller of Customer Data under the Agreement. As for the property element of the standard, Article 8.1 of the G Suite Agreement states that the Customer "Owns all Intellectual Property Rights to the Data". The question then is whether "intellectual property rights" is sufficiently equivalent to the term "property right" in order to satisfy the objectives of the statute? The World Intellectual Property Organization ("WIPO") states that "intellectual property rights" are the same as any other property right as they would be applied to intangible content such as pupil records, and has, at its core, an exclusive right to the property. We think these terms are sufficiently related to be termed equivalent and in compliance with the statute.

2. Does the G Suite Agreement Contain a Description of the Means by which Pupils may Retain Possession and Control of their own Pupil-Generated Content, if Applicable, Including Options by which a Pupil may Transfer Pupil-Generated Content to a Personal Account?

The G Suite Agreement does not specifically state that a pupil may transfer pupil-generated content to a personal account. However, the logic of the G Suite Agreement's language leads to such a result. First, the definition of Customer Data includes all data generated by an End User (which, here, constitutes pupils); any clause regarding Customer Data shall, by extension, also apply to pupil-generated content. (G Suite Online Agreement, section 16).

Google agrees to move and export Customer data in two ways. The first is by request of the Customer, or defined by Google as the End User (DPA, section 8.1). The second is request of the End User, or the student (Id at 8.2). When the student is making the request, the student must work through the LEA. Google is merely the facilitator, allowing access and fulfilling the request technically. Control over the decisions to transfer remains with the LEA in both cases. This procedure is consistent with the idea that it is the LEA that has control over and supervises the management of data, which we believe is the intent of FERPA and AB 1584. (We will later call this a "reserved power"). As a result, the G Suite Agreement would meet the burden of general compliance with AB 1584 for pupil-generated content. Google's defined role would therefore be that of a facilitator of data transfers, implementing the decisions of the LEA. We will discuss this in more detail below.

3. Does the G Suite Agreement contain a prohibition against a Third-Party using any Information in the Pupil record for any Purpose Other than Those Required or Specifically Permitted by the Contract?

The G Suite Agreement complies with this requirement in a relatively straightforward manner. Section 5.3 of the G Suite Online Agreement states as follows:

"Processing Restrictions. Google will only process Customer Data in accordance with the Agreement and will not process Customer Data for any other purpose."

Although this passage does not use exactly the same language as that found in AB 1584, we believe the passage satisfies the underlying purpose of the requirement.

4. Does the G Suite Agreement Contain a Description of the Procedures by Which a Parent, Legal Guardian, or Eligible Pupil may Review Personally Identifiable Information in the Pupil's Records and Correct Erroneous Information?

In many ways this section is one of the core concerns of FERPA and is dealt with in some length (U.S.C. 1232g (a)(1) 1232 (a) (1) (D); Regulations section 99.10-22). It is also a central concern of AB 1584 and its statutory framework. Compliance with this section of AB 1584 and FERPA is therefore vital to a finding of overall statutory compliance. Our answer will depend on what this section requires of a private vendor.

As mentioned above, the term "Customer Data" as defined by the G Suite Online Agreement includes personally identifiable information from education records. Sections 8.1 and 8.2 of the DPA state that Google will provide the LEA with access to and the ability to correct Customer Data, and that any request by an "End User" (e.g. student or parent) for records will be directed to the LEA. End User is defined as "individuals [the LEA] permits to use the Services,"[3] which does not include parents or legal guardians. Further, there are no explicit procedures in place for a parent or legal guardian to access, view, or correct a student's personally identifiable

[3] See G Suite Agreement, section 16, defining "End User."

information, which prevents the Agreements from strictly complying with AB 1584.[4] (Page 2 of the Privacy Notice has a section called "Parent Review and Deletion of Information", but it is unclear whether this section was drafted to address this requirement of AB 1584 and in any event posits a passive role for Google.)

The question then becomes, is Google required by AB 1584 to state and follow a complete procedure whereby personally identifiable information can be reviewed and erroneous information corrected? We think the answer requires an interpretation of that section of AB 1584, using traditional rules of statutory construction, and how statutes must be read within a larger context. California Education Code section 49073.1 is part of a large Article of the California Education Code (Article 5, sections 49073 to 49079.5), which itself is part of a larger Chapter of the Education Code (Chapter 6.5, from sections 49060 to 49086). To understand one subpart of California Education Code section 49073.1 it is not enough to read it in isolation, it must be read with in the context of the larger statutory scheme in which it is found. (*In re Marriage of Harris* (2004) 17 Cal. Rptr. 3d 842 (2004); *Welch v. Oakland Unified School District* (2001) 111 Cal. Rptr. 2d 374.)

For all of its importance, AB 1584 is a relatively limited section of an overall statutory enactment that comprehensively adjusts the manner in which pupil records are to be kept, and whether they will be protected from, or subject to disclosure. The manner in which student records are reviewed or modified is not found in California Education Code section 49073.1. It is addressed in other sections of Chapter 6.5. For example, it is undisputed that a grade is a student record. The manner in which a student grade is changed is left entirely to the LEA itself (California Education Code section 49066). The right to challenge a record and to have it corrected is spelled out in some detail in California Education Code section 49070. The process of review and modification is a multi-part process involving the LEA's superintendent and the Governing Board.

We see nothing in California Education Code section 49073.1 that would alter the status quo established in California Education Code sections 49066 or 49070, which leaves the power and authority for reviewing and correcting student records to persons other than the digital provider. The statutes also indicate that the digital providers will not have a substantive role. The reader is directed to California Education Code section 49076, which can be viewed as a companion statute to California Education Code section 49073.1.

Section 49076 specifies the conditions under which pupil records can be disclosed without parental consent. California Education Code section 49076 (a)(2)(G) is the analog to FERPA's "School Official" exception. Pupil records can be outsourced to digital providers like Google, but only if a series of conditions are met. These include the condition that a vendor's right of access to the data shall not include the right to add, delete, or alter data without the written permission of the agency holding the data (California Education Code section 49076 (a)(4)(D)).

[4] An "eligible pupil" would fall within the definition of End User, and therefore the AB 1584, required description of a process is satisfied in this regard.

Google therefore cannot have any substantive role in the review, modification or deletion of student records and be in compliance with the statute. This is a statutorily "reserved power" of the LEA, a role that cannot be outsourced. How then do we harmonize the language of California Education Code sections 49076 and 49073.1? We think that this harmony is achieved by reading California Education Code section 49073.1 (a)(4) in a narrow manner. We interpret the section to mean, that a digital provider must agree to (1) provide access to the "Pupil Records" in question and (2) modify or delet them when requested to do so by the LEA.

We think the result is the same where FERPA is concerned. The numerous sections show that it is the educational agency that oversees each step of the record review process, from preparing policies and procedures (Section 1232g (a), to the conduct of the hearing (Section 99.21 (a)). In this setting, Google is not supposed to have a substantive role in the FERPA record-review process.

The Privacy Policy (at page 3), meets this technically based standard. Google's Privacy Policy promises user access to records and to update or delete the data, so long as this is consistent with "legal purposes." In section 7.1 and 8.1 of the G Suite Online Agreement, a Customer or User has the ability to correct, block and delete the Customer data in a manner consistent with the functionality of the Services. We find these sections comply with AB 1584.

5. Does the G Suite Agreement Contain a Description of the Actions Google will Take, Including the Designation and Training of Responsible Individuals, to Ensure the Security and Confidentiality of Pupil Records?

The wording of the G Suite Online Agreement by itself could result in a misapprehension as to how robust its security measures actually are. Its wording is cautious and "lawyerly." Each party (including Google), will take "reasonable care" to protect data from unauthorized use. (G Suite Online Agreement, section 2.6) Google also appears to agree that it will protect a Customer's data to the same extent Google protects its own data. (G Suite Online Agreement, section 7.1) This "Golden Rule" data protection is somewhat cryptic and may not appear convincing to some readers.

However, a review of the other G Suite Agreement documents shows that Google takes substantial efforts to protect student data. For example, in the DPA, at section 6.1 and Appendix 2, "Security Measures" state in some considerable detail the training and security measures Google undertakes to protect student data. These measures are further enumerated in ISO 27018 (which we have already discussed) and in the Whitepaper issued by Google discussing its security measures. When taken together, there is no doubt that Google provides adequate training and security measures to protect student data.

6. Does the G Suite Agreement Contain a Description of the Procedures for Notifying an Affected Parent, Legal Guardian, or Eligible Pupil in the Event of an Unauthorized Disclosure of the Pupil's Records?

Google's compliance with AB 1584's provisions regarding an unauthorized disclosure of Pupil Records can be found in two sections of the DPA. Section 6.3 states that Google will promptly notify customers of the Data Incident and take reasonable steps to minimize the harm and secure Customer Data. In addition, the DPA expressly incorporates the requirements of ISO 27018:2014 in its security practices (Section 6.4). Section 9.1 of ISO 27018 states that Google should specify that the date of the incident should be listed, the type of data compromised and the efforts taken to address the problem. Section 9.1 implies that this information should be transmitted to the Customer. (Google should clarify that this is the case.) We therefore think that the G Suite Agreement complies with this strand of the AB 1584.

7. Does the G Suite Agreement Contain a Certification that a Pupil's Records Shall not be Retained or Available to Google upon Completion of the Terms of the Contract, as well as a Description of how that Certification will be Enforced?

Oddly enough, California Education Code section 49073.1 discusses only the issue of record retention by the vendor, not the return of the data to the customer. This same "one-legged" approach for requiring data destruction but not its return, can also be found in FERPA (See 1232 (b) (1) (F)). The G Suite Agreement addresses both data retention and return. Upon termination, Google allows the data to be exported back to the LEA (G Suite Online Agreement, section 12.3). If the LEA takes no such action, the data will be deleted by Google after 189 days (DPA, section 7.1). Google meets this standard.

8. Does the G Suite Agreement Contain a Description of How the LEA and the Third-Party Will Jointly Ensure Compliance with FERPA?

This section is something of a "catch-all" because it appears to import into AB 1584 the entirety of the substantive requirements of FERPA. The question then becomes, does FERPA require contract provisions in addition to those listed in AB 1584? We conclude that for all practical purposes, the answer is "no." AB 1584 shifts the focus of analysis from the LEAs to what must be in the contracts between the LEAs and digitals providers. (It also contains data security and breach notifications that do not appear to be contained in FERPA).

FERPA uses a somewhat different terminology to justify the "out sourcing" of Pupil Records to a third-party. This is the so-called "School Official" exception. (20 U.S.C. 1232 g (b)(1)(A); 34 C.F.R. section 99.31(a)(1); 34 C.F.R. section 99.31 (a)(1)(i)(B)). One of the core requirements of the "School Official" exception is that the vendor remains under the direct control of the assigning LEA. (C.F.R. 99.31 (B)(1)).

The G Suite Agreement meets the "School Official" standard in two ways. First, the G Suite Online Agreement states that Google is receiving the data from a school district as a "School Official", where applicable. (G Suite Online Agreement, section 7.4). Second, numerous sections throughout the various contract documents make it clear that data held by Google remains under the supervision and control of the LEA. (See, e.g. G Suite Online Agreement sections 2.3, 2.4 and 8.1; Privacy Policy pager 3). We believe these sections show compliance with FERPA and this AB 1584 requirement.

9. Is Google Prohibited from Engaging in "Targeted Advertising?"

In order to analyze this requirement we need to arrive at a precise definition and application of the term "targeted advertising." If "targeted advertising" means advertising undertaken by Google without the consent of the Customer, then the G Suite Online Agreement meets this requirement when it states: "Google does not serve Ads in the Services or use Customer data for Ads purposes." (Section 1.4).

However, things become more nuanced when Google notes that Customer (or the LEA), can elect to participate in services or products that allow targeted advertising, primarily as means of making money. This program is called "Google AdSense." It is uncertain whether the "AdSense" program complies with this section. However, Google has not allowed the addition of new sites to the AdSense Program since 2013, and this program should become a legacy issue. For new customers, this requirement has been met.

10. Does Google Represent That Its Subprocessors Will Adhere to AB 1584?

Surprisingly, AB 1584 does not contain a specific section requiring Subprocessors of digital vendors also to comply with AB 1584. (Subprocessors can also sometimes be referred to in the industry as Subcontractors.) However, SOPIPA does contain such an express requirement, and can be found at California Business and Professions Code section 22584 (b) (4) (E). It can also be argued persuasively that the purpose of AB 1584 would be frustrated unless Subprocessors were also bound by its provisions.

The documents that comprise the G Suite Agreement have several provisions binding Google's Subprocessors to the protections and responsibilities of the G Suite Online Agreement (DPA, sections 11.1 and 11.2) In addition Google describes the process by which Subprocessors are vetted:

"Prior to 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 always to the requirements set out in section 11.2 (Subprocessing Restrictions) of this DPA, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms. (Appendix 2, section 5)."

We believe these contract sections and the audit process they describe, demonstrate Google's Agreement to bind Subprocessors to the terms of the G Suite Agreement and AB 1584.

Conclusion

Based on our foregoing analysis, we have concluded that the G Suite Agreement, as currently offered and including multiple documents, is in conformance with both AB 1584 and FERPA requirements. Please contact me if you have any further questions.

Sincerely,

FAGEN FRIEDMAN & FULFROST, LLP

Mark S. Williams

Enclosures Exhibits A-J
MSW:lct
00618-00001/1617856.1

GOOGLE EXHIBITS

EXHIBIT A

MGMT. SYS.
RvA C 466

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

CERTIFY EY POINT

Certificate

Certificate number: 2012 - 001

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Google Inc.*

located in Mountain View, California, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2005

Issue date of certificate: May 11, 2012
Re-issue date of certificate: April 14, 2014
Expiration date of certificate: April 18, 2015

Ernst & Young CertifyPoint B.V. will, according to the certification agreement (dated May 11, 2012), perform surveillance audits and acknowledges the certificate until the expiration date of the certificate.

**This certificate is applicable for the key components, assets and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in the 'Google ISO 27001 Implementation Manual,' version 2.4, approved on March 10, 2014.*

drs. R. Toppen RA
Director EY CertifyPoint

MGMT. SYS.
RvA C 466

Google Inc.
Scoping for certificate 2012-001

The functional scope of this ISO/IEC 27001:2005 Certification is bounded by the Google Apps for Business (and Google Apps for Education), Google Cloud Platform, Google Helpouts, Google Plus, Google Now, Google Analytics and Analytics Premium offerings and the data contained or collected by those offerings and specified facilities. The ISMS is centrally managed out of Google Inc. headquarters in Mountain View, California USA.

The in-scope applications, systems, people and processes are globally implemented and operated by teams out of an explicit set of offices and data centers that comprise the functional scope as specifically defined in the 'Google ISO 27001 Implementation Manual.' The listing below indicates which offerings by product are included in the scope of the ISMS.

- **Google Apps for Business and Google Apps for Education:** Gmail, Calendar, Drive, Docs, Sheets, Slides, Talk, Vault, Sites, Groups, Tasks, Contacts, Admin Console (formerly Control Panel or CPanel), Directory API (formerly Directory Sync tool and Provisioning API), Reports API (formerly Reporting and Audit API), SAML-based SSO API;
- **Google Cloud Platform:** Compute Engine, App Engine, Cloud SQL, Cloud Storage, Cloud Datastore, BigQuery;
- **Google Helpouts;**
- **Google Plus:** Plus, Hangouts;
- **Google Now**; and
- **Google Analytics and Google Analytics Premium.**

The ISMS mentioned in the above scope is restricted as defined in the 'Google ISO 27001 Implementation Manual' document, version 2.4, signed on March 10, 2014, by the Senior Manager Engineering Compliance as well as the 'Google ISO 27001 Scope and Bounds Assertion' (formal ISMS location listing document), version 1.0, signed on April 7, 2014 by the Senior Manager Engineering Compliance.

This scope (edition: April 14, 2014) is only valid in connection with certificate 2012-001.

MGMT. SYS.
RvA C 466

Certificate

Certificate number: 2012-001
Certified by EY CertifyPoint since:
May 11, 2012

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Google, Inc.*

located in Mountain View, California, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: April 15, 2015
Expiration date of certificate: April 14, 2018

EY CertifyPoint will, according to the certification agreement dated February 13, 2015, perform surveillance audits and acknowledge the certificate until the expiration date of the certificate.

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated March 5, 2015.*

drs. R. Toppen RA
Director EY CertifyPoint

MGMT. SYS.
RvA C 466

Google, Inc.
Scope for certificate 2012-001

The scope of this ISO/IEC 27001:2013 certification is bounded by the Google Apps for Work and Google Apps for Education, Google Cloud Platform, Google+, Google Life Sciences, Google Now, Google Analytics and Google Analytics Premium offerings and the data contained or collected by those offerings and specified facilities. The Information Security Management System (ISMS) is centrally managed out of the Google, Inc. headquarters in Mountain View, California, United States of America.

The in-scope applications, systems, people and processes are globally implemented and operated by teams out of an explicit set of offices and data centers that comprise the functional scope as specifically defined in the 'Google ISO 27001 Implementation Manual.' The listing below indicates which offerings by product are included in the scope of the ISMS.

- **Google Apps for Work and Google Apps for Education**: Gmail, Calendar, Drive, Docs, Sheets (including Forms), Slides, Talk, Hangouts, Vault, Sites, Groups, Tasks, Contacts, Admin console, Directory API, Reports API, SAML-based SSO API, Apps Script, Classroom, Inbox by Gmail;
- **Google Cloud Platform**: Compute Engine, App Engine, Cloud SQL, Cloud Storage, Cloud Datastore, BigQuery, Genomics;
- **Google+**;
- **Google Life Sciences:** Baseline Study, BioQuery, Google Life Sciences Study Kit;
- **Google Now**; and
- **Google Analytics and Google Analytics Premium.**

The ISMS mentioned in the above scope is restricted as defined in the 'Google ISO 27001 Implementation Manual', version 2.8, signed on March 5, 2015, by the Senior Manager of Engineering Compliance, as well as the 'Google ISO 27001 Scope and Bounds Assertion' (formal ISMS location listing document), version 1.2, signed on January 23, 2015, by the Senior Manager of Engineering Compliance.

This scope (edition: March 5, 2015*) is only valid in connection with certificate 2012-001.*

Certificate

Certificate number: 2016-004
Certified by EY CertifyPoint since:
April 15, 2016

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Google, Inc.*

located in Mountain View, California, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27017:2015

Issue date of certificate: April 15, 2016
Expiration date of certificate: April 14, 2018

EY CertifyPoint will, according to the certification agreement dated February 13, 2015, perform surveillance audits and acknowledge the certificate until the expiration date of this certificate or the expiration of the related ISMS certificate with certificate number [2012-001].

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for cloud security as stated in the Statement of Applicability version 2.6, dated January 19, 2016.*

drs. R. Toppen RA
Director EY CertifyPoint

Google, Inc.
Scope for certificate 2016-004

The scope of this ISO/IEC 27017:2015 certification is bounded by the products and their offerings as listed below, along with the data contained or collected by those offerings.

➢ **Google Apps for Work, Google Drive for Work (Google Apps Unlimited) and Google Apps for Education,** this includes:

Google Apps Products:

- Gmail
- Calendar
- Drive
- Docs
- Sheets
- Forms
- Slides
- Talk
- Hangouts
- Vault
- Sites
- Groups
- Tasks
- Contacts
- Admin console
- Apps Script
- Classroom (Only for Google Apps for Education)
- Inbox by Gmail
- Keep

Google Product APIs:

- GMail REST API
- Drive REST API
- Calendar API
- Contacts API
- Tasks API
- Sites API
- Sheets API
- Apps Activity API

Google Apps Admin SDK APIs:

- Admin Settings API
- Domain Shared Contacts API
- Directory API
- Reports API
- SAML-based SSO API
- Apps Email Audit API
- Calendar Resource API
- Email Settings API
- Groups Migration API
- Groups Settings API
- Enterprise License Manager API
- Reseller API

Google, Inc.
Scope for certificate 2016-004

- **Google Cloud Platform:**
  - App Engine
  - Compute Engine
  - Cloud SQL
  - Cloud Storage
  - Cloud Datastore
  - BigQuery
  - Genomics
  - Cloud Dataflow
  - Cloud Bigtable
  - Container Engine
  - Cloud Dataproc
  - Container Registry

The Information Security Management System (ISMS) is centrally managed out of the Google, Inc. headquarters in Mountain View, California, United States of America. The ISMS mentioned in the above scope is restricted as defined in the 'Google ISO 27001 Scope and Bounds Assertion' (formal ISMS location listing document), version 1.4, signed on January 19, 2016, by the Senior Manager of Engineering Compliance.

EXHIBIT B

Certificate

Certificate number: 2016-005
Certified by EY CertifyPoint since:
April 15, 2016

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Google, Inc.*

located in Mountain View, California, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27018:2014

Issue date of certificate: April 15, 2016
Expiration date of certificate: April 14, 2018

EY CertifyPoint will, according to the certification agreement dated February 13, 2015, perform surveillance audits and acknowledge the certificate until the expiration date of this certificate or the expiration of the related ISMS certificate with certificate number [2012-001].

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security and protection of personally identifiable information (PII) as stated in the Statement of Applicability version 2.6, dated January 19, 2016.*

drs. R. Toppen RA
Director EY CertifyPoint

Google, Inc.
Scope for certificate 2016-005

The scope of this ISO/IEC 27018:2014 certification is bounded by the products and their offerings as listed below, along with the data contained or collected by those offerings.

➢ **Google Apps for Work, Google Drive for Work (Google Apps Unlimited) and Google Apps for Education,** this includes:

Google Apps Products:

- Gmail
- Calendar
- Drive
- Docs
- Sheets
- Forms
- Slides
- Talk
- Hangouts
- Vault
- Sites
- Groups
- Tasks
- Contacts
- Admin console
- Apps Script
- Classroom (Only for Google Apps for Education)
- Inbox by Gmail
- Keep

Google Product APIs:

- GMail REST API
- Drive REST API
- Calendar API
- Contacts API
- Tasks API
- Sites API
- Sheets API
- Apps Activity API

Google Apps Admin SDK APIs:

- Admin Settings API
- Domain Shared Contacts API
- Directory API
- Reports API
- SAML-based SSO API
- Apps Email Audit API
- Calendar Resource API
- Email Settings API
- Groups Migration API
- Groups Settings API
- Enterprise License Manager API
- Reseller API

Google, Inc.
Scope for certificate 2016-005

➢ **Google Cloud Platform:**
- App Engine
- Compute Engine
- Cloud SQL
- Cloud Storage
- Cloud Datastore
- BigQuery
- Genomics
- Cloud Dataflow
- Cloud Bigtable
- Container Engine
- Cloud Dataproc
- Container Registry

The Information Security Management System (ISMS) is centrally managed out of the Google, Inc. headquarters in Mountain View, California, United States of America. The ISMS mentioned in the above scope is restricted as defined in the 'Google ISO 27001 Scope and Bounds Assertion' (formal ISMS location listing document), version 1.4, signed on January 19, 2016, by the Senior Manager of Engineering Compliance.

This scope (edition: **April 15, 2016***)*
is only valid in connection with certificate 2016-005.

INTERNATIONAL STANDARD

ISO/IEC 27018

First edition
2014-08-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Reference number
ISO/IEC 27018:2014(E)

EXHIBIT C

Google™

Service Organization Controls (SOC) 3 Report

Report on the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services Relevant to Security, Availability, Processing Integrity, and Confidentiality

For the Period 1 May 2014 to 30 April 2015

1600 Amphitheatre Parkway
Mountain View, California 94043

Google™

Tel: 650.623.4000
Fax: 650.618.1806
www.google.com

Google's Management Assertion Regarding the Effectiveness of Its Controls Over the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services (System) Based on the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, and Confidentiality

Google Inc. (the Company) maintained effective controls over the security, availability, processing integrity and confidentiality of its Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services (System) to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification;
- the System was available for operation and use, as committed and agreed;
- the System processing was complete, accurate, timely, and authorized; and
- the System information designated as confidential was protected as committed or agreed

during the period 1 May 2014 through 30 April 2015 based on the security, availability, processing integrity, and confidentiality principles set forth in the American Institute of Certified Public Accountants' (AICPA) TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Our attached System Description of the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services (System) identifies the aspects of the System covered by our assertion.

GOOGLE Inc.

15 July 2015

EY
Building a better
working world

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Google Inc.:

We have examined management's assertion that Google Inc., during the period 1 May 2014 through 30 April 2015, maintained effective controls to provide reasonable assurance that:

- the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services System was protected against unauthorized access, use, or modification;
- the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services System was available for operation and use, as committed or agreed;
- the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services System processing is complete, valid, accurate, timely, and authorized;
- information within the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services System designated as confidential is protected as committed or agreed

based on the criteria for security, availability, processing integrity and confidentiality in the American Institute of Certified Public Accountants' (AICPA) TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Google Inc.'s management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of Google Inc.'s relevant security, availability, processing integrity and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or deterioration in the degree of effectiveness of the controls.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, processing integrity and confidentiality.

Ernst + Young LLP

15 July 2015

Description of the Google Apps for Work, Google Drive for Work (Google Apps Unlimited), Google Apps for Education, Google Cloud Platform and Other Google Services System

Google Overview

Google Inc. ("Google") is a global technology service provider focused on improving the ways people connect with information. Google's innovations in web search and advertising have made Google's web site one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world's largest online index of web sites and other content, and makes this information freely available to anyone with an Internet connection. Google's automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google offers Internet-based services and tools that user entities can access to communicate, collaborate, and work more efficiently. The following Google product offerings automatically saves all work performed by user entities in the cloud and enables user entities to work securely, regardless of where they are in the world and what device they are using.

Google Apps for Work, Google Drive for Work (Google Apps Unlimited), and Google Apps for Education, hereafter described collectively as "Google Apps," include:

Products	**Google Apps for Work**	**Google Drive for Work (Google Apps Unlimited*)**	**Google Apps for Education**
Gmail	✓	✓	✓
Google Calendar	✓	✓	✓
Google Classroom			✓
Google Contacts	✓	✓	✓
Google Docs	✓	✓	✓
Google Drive	✓	✓	✓
Google Forms	✓	✓	✓
Google Groups	✓	✓	✓
Google Hangouts	✓	✓	✓
Google Sheets	✓	✓	✓
Google Sites	✓	✓	✓

Products	Google Apps for Work	Google Drive for Work (Google Apps Unlimited*)	Google Apps for Education
Google Slides	✓	✓	✓
Google Talk	✓	✓	✓
Google Tasks	✓	✓	✓
Google Vault	✓	✓	✓
Google Apps Admin Console	✓	✓	✓
Google Apps Script	✓	✓	✓
Admin SDK Application Programming Interfaces (APIs)	✓	✓	✓
Product APIs	✓	✓	✓
Inbox by Gmail	✓	✓	✓

*Google Apps Unlimited is the premium version of Google Apps. In addition to the features available in Google Apps for Work, it includes unlimited storage space and Google Apps Vault for everyone in user's organization. It also offers additional Drive administration, auditing, and reporting features.

Google Cloud Platform allows businesses and developers to build and run their applications on Google's Cloud using the following services, hereafter described collectively as "Google Cloud Platform":

- Google App Engine
- Google BigQuery
- Google Cloud Datastore
- Google Cloud SQL
- Google Cloud Storage
- Google Compute Engine
- Google Genomics

Google social and communication services, hereafter described collectively as "Other Google Services," include:

- Google Now
- Google+

Google's product offerings including Google Apps, Google Cloud Platform and Other Google Services provide the unique advantage of leveraging the resources of Google's core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

Google Apps, Google Cloud Platform and Other Google Services are targeted to small businesses, medium businesses, and large corporations alike. These products provide what business organizations typically require, including the following:

- Multi-user collaboration
- No special hardware or software required by the enterprise
- Security and compliance features
- Seamless upgrades

The products are comprised of communication, productivity, collaboration and security tools that can be accessed from virtually any location with Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with an Internet connection.

The Google Apps, Google Cloud Platform and Other Google Services covered in this system description consist of the following services:

Gmail

Gmail is a cloud-based email service providing web browser and mobile interfaces. Gmail provides customizable email addresses which include the user entity's own domain, mail search tools and integrated chat. Users can compose and manage email, filter for spam and viruses. It is fully integrated with other Google services such as Calendar, Groups and Drive.

Google Calendar

Google Calendar is a cloud-based calendaring service providing web browser and mobile interfaces. Calendar is an application that enables individuals and corporations to coordinate and schedule people, meeting rooms and other resources. Users can create events, send invitations, share schedules and track RSVPs. It is fully integrated with other Google services such as Gmail, Drive and Hangout.

Google Classroom

Google Classroom is cloud-based school communication and assignment management tool. It allows users to create and join classroom groups as teachers and students, distribute and grade assignment as a teacher, or view and submit assignments as a student. Classroom is only available to Apps for Education users.

Google Contacts

Google Contacts is a cloud-based contacts service providing web browser and mobile interfaces. It allows users to import, store and organize contact information about people and businesses with whom they communicate. Not only can each contact contain basic information such as names, email addresses and phone numbers, but also can include extended information like physical address, employer, department or job title. Users can also create personal groups of contacts to email many people at once. It is fully integrated with other Google services such as Gmail, Drive and Groups.

Google Docs

Google Docs is an online word processor that lets users create and format text documents and collaborate with other users in real time. Documents can be private or shared, and multiple people can edit the same document at the same time. Comments can also be left in the document, and documents can be exported to other file formats.

Google Drive

Google Drive is a cloud-based storage solution, where users can create, share, collaborate and keep their files. It provides the sharing controls for files and folders, including Google Docs, Sheets and Slides, as well as any other file type. Drive comes with desktop and mobile apps, making it much easier to upload, synchronize and access files from any device. It is fully integrated with other Google services such as Groups, Hangouts and Gmail.

Google Forms

Google Forms is an online data collection tool that lets users collaboratively build and distribute surveys, polls and quizzes. Google Forms provides real-time analysis of structured form response data through integration with Google Sheets.

Google Groups

Google Groups is a cloud-based rostering service providing web browser and mobile interfaces. It allows online creation and management of user groups. Groups users can engage in discussions about a specific subject; organize meetings, conferences or social events among members of a group; find people with similar hobbies, interests or background; share file and calendar events; read groups posts through email, the online interface or both; and more. It is fully integrated with other Google services such as Gmail, Drive, and Calendar.

Google Hangouts

Google Hangouts is a real-time communication and messaging application that allows users to send and receive messages, photos and videos and make one-to-one and group video calls of up to 15 users at a time. It is available on mobile and desktop devices and is fully integrated with Google products such as Gmail, Drive and Calendar.

Google Sheets

Google Sheets is an online spreadsheet application that lets users create and format spreadsheets and simultaneously work with other users. Spreadsheets can be private or shared, and multiple people can edit the same spreadsheet at the same time. Comments can also be left in the spreadsheet, and spreadsheets can be exported to other file formats.

Google Sites

Google Sites is a cloud-based publishing service providing web browser and mobile browser interfaces. It allows the creation of site pages to share and collaborate on documents, videos, schedules and more. It can be published as an internal or an external facing web site. It is fully integrated with other Google services such as Drive and Groups.

Google Slides

Google Slides is an online presentation application that allows users to show off their work in a visual way and present to audiences. Presentations can be private or shared, and multiple people can edit the same presentation at the same time. Comments can also be left in the presentation, and presentations can be exported to other file formats.

Google Talk

Google Talk is an application that enables text, video and voice communications. Users can initiate a chat, invite friends to a chat and place phone calls to any landline or mobile phone number included in Gmail contacts.

Google Tasks

Google Tasks is an online application that allows users to create task lists and tasks. It is integrated with Gmail and the Google Calendar applications.

Google Vault

Google Vault is corporate solution that provides additional storage and searching tools to manage critical information and preserving important corporate data. Vault helps protect user entities with easy-to-use searches so they can quickly find and preserve data to respond to unexpected customer claims, lawsuits or investigations during the electronic discovery (eDiscovery) process. Additionally, Vault gives Google Apps user entities the extended management and information governance capabilities to proactively archive, retain and preserve Gmail and on-the-record chats. With the ability to search and manage data based on terms, dates, senders, recipients and labels, Vault helps user entities find the information they need, when they need it.

Google Admin Console

Google Admin Console, formerly Google Apps Control Panel, is a cloud-based user and device administrative service used to configure the different applications, perform user management, utilize admin tools, etc. Users can initiate transactions such as creating user accounts to give users access to various Google Apps services, and managing Google services settings.

Google Apps Script

Google Apps Script is a JavaScript cloud scripting language that provides easy ways to automate tasks across Google products and third party services. Users can define the set of transactions their scripts can initiate and process.

Admin SDK

The Administrative Tools for Google Apps within the Admin SDK are used to manage users, groups, devices and apps, create custom usage reports and migrate email and groups to Google Apps.

- *Admin Settings API*
  The Admin Settings API allows administrators of Google Apps domains to retrieve and change the settings of their domains in the form of Google Data API feeds. These domain settings include many of the features available in the Google Apps Admin Console.

- *Directory API*
  Google Apps and reseller administrators can use the Directory API to manage Mobile and Chrome OS devices, groups, group aliases, members, organizational units, users and user aliases.

- *Domain Shared Contacts API*
  The Domain Shared Contacts API allows client applications to retrieve and update external contacts that are shared to all users in a Google Apps domain.

- *Apps Email Audit API*
  The Email Audit API allows Google Apps administrators to audit a user's email, email drafts and archived chats.

- *Calendar Resource API*
  The Calendar Resource API allows Google Apps administrators to retrieve and manage the Google Calendar resources of their domains in the form of Google Data API feeds.

- *Email Settings API*
  The Email Settings API allows website administrators to offer their users co-branded versions of a variety of personalized Google applications, such as Google mail.

- *Groups Migration API*
  The Groups Migration API lets account-level administrators migrate emails from public folders and distribution lists to Google Groups discussion archives.

- *Groups Settings API*
  The Groups Settings API allows account-level administrators to manage the group settings for their Google Apps account.

- *Enterprise License Manager API*
  The Enterprise License Manager API allows administrators to assign, update, retrieve and delete user licenses.

- *Reports API*
  The Reports API lets the account administrators customize usage reports.

- *Reseller API*
  The Reseller API can be used by authorized reseller administrators and reseller's service integrators to place customer orders and manage Google Apps monthly post-pay subscriptions.

Product APIs

- *Gmail Representational State Transfer (REST) API*
  The Gmail REST API is a RESTful API that can be used to access Gmail mailboxes and send mail. For most web applications (including mobile apps), the Gmail API is the best choice for authorized access to a user's Gmail data for Google Apps users.

- *Drive REST API*
  The Drive REST API is a RESTful API that can be used to Create, Open, Search and Share contents in Google Drive for Google Apps users.

- *Calendar API*
  The Calendar API is a RESTful API that allows client applications to access and edit Google Calendar data for Google Apps users.

- *Contacts API*
  The Contacts API can be used to create new contacts, edit or delete existing contacts and query for contacts that match particular criteria for Google Apps users.

- *Tasks API*
  The Tasks API provides access for searching, reading and updating Google Tasks content and metadata for Google Apps users.

- *Sites API*
  The Sites API allows client applications to access, publish, and modify content within a Google Site, create and delete sites. The API is available to both Google Account and Google Apps users.

- *Sheets API*
  The Sheets API enables developers to create applications that read and modify the data in Google Sheets.

- *Apps Activity API*
  The Apps Activity API allows client applications to retrieve information about a user's Google Apps activity. Currently, the API supports retrieving activity from the Google Drive service regarding changes to a user's Google Drive files. This provides additional functionality on top of the existing Drive API for an app to perform tasks such as displaying activity on a user's files, tracking changes to specific files or folders and alerting a user to new comments or changes to files.

Inbox by Gmail

Inbox by Gmail is the Gmail next generation inbox designed to help people keep track of everything they need to get back to at a later time. It is available on Android, iOS and web.

Google App Engine

Google App Engine is Google's Platform-as-a-Service (PaaS) offering used to build web applications on Google's infrastructure. Google App Engine enables users to build and host web apps on the same systems that power Google applications. App Engine offers fast development and deployment; simple administration, with no need to worry about hardware, patches or backups; and effortless scalability. Google App Engine users can define the set of transactions their applications can initiate and process.

Google BigQuery

Google BigQuery is a fully managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes. It enables companies to import multi-terabyte datasets, query interactively and securely share the results within their organization.

Google Cloud Datastore

Google Cloud Datastore provides a managed, NoSQL, schema-less database for storing non-relational data. Cloud Datastore automatically scales with your users and supports transactions, as well as robust queries.

Google Cloud SQL

Google Cloud SQL stores and manages data using a fully-managed, relational MySQL database. It is a highly available hosted SQL-based storage solution that allows users to create, configure and use relational databases that live in Google's infrastructure. Cloud SQL is tightly integrated with Google App Engine, Compute Engine, Cloud Storage and other Google services.

Google Cloud Storage

Google Cloud Storage is a service for storing and accessing user data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities. Users can define the set of transactions their applications can initiate and process.

Google Compute Engine

Google Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. Google Compute Engine allows users to solve large-scale processing and analytic problems on Google's computing, storage and networking infrastructure. Users can launch virtual machines on-demand, manage network connectivity using a simple but flexible networking solution and access a variety of data storage alternatives from their virtual machines.

Google Genomics

Google Genomics provides an API to store, process, explore and share DNA sequence reads, reference-based alignments and variant calls, using Google's cloud infrastructure.

Google Now

Google Now provides personalized and contextual suggestions and recommendations via mobile, desktops and wearable devices. Google Now delivers customized and highly relevant information users care about automatically based on the settings they choose. Simple cards bring the information such as weather, traffic and stock prices that users want to help manage the users' day.

Google+

Google+ is a social networking platform that is fully integrated with other Google products. Users create and are able to manage their own Google+ profile. Google+ allows users to create and share content with each other. It also enables users to select and organize people into groups for optimal sharing across various Google products and services.

Infrastructure

Google Apps for Work, Google Apps, Google Cloud Platform and Other Google Services run in a multi-tenant, distributed environment. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed across a shared infrastructure. For Google Apps, Google Cloud Platform and Other Google Services, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Structured data (e.g., emails, docs, sheets, etc.) is then stored in large distributed databases, built on top of this file system. Alternate storage procedures are documented and in place for backing up and recovering customer data. Data is chunked and replicated over multiple systems such that no one system is a single point of failure. Data chunks are given random file names and are not stored in clear text so they are not humanly readable. Gmail backups are periodically performed to support the availability of user entity data. Gmail data restore tests are continuously performed on a rolling subset of data to confirm the ability to recover customer data from backup tapes.

Data Centers and redundancy

Google's computing clusters are architected with resiliency and redundancy in mind, helping minimize single points of failure and the impact of common equipment failures and environmental risks. Dual circuits, switches, networks, and other necessary devices are utilized to provide redundancy. Facilities infrastructure at the data centers has been designed to be robust, fault tolerant, and concurrently maintainable.

Critical data is replicated to at least two (2) data centers and provides high availability by dynamically load balancing across those sites. Google applications are designed to anticipate and tolerate failures of components. Such protections are also designed to ensure that services are available in the event of natural disasters.

Authentication and access

Strong authentication and access controls are implemented to restrict administrative access to Google Apps, Google Cloud Platform and Other Google Services production systems, internal support tools, and customer data. Machine-level access restriction relies on a certificate based distributed authentication service, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. All data traffic is encrypted between Google production facilities.

Google follows a formal process to grant or revoke employee access to Google resources. Both user and internal access to customer data is restricted through the use of unique user IDs. Unique user IDs, strong passwords, One-Time-Passwords (OTP) and periodic reviews of access lists are performed to help ensure access to customer data is appropriate and authorized.

Data

Google provides controls at each level of data storage, access, and transfer. Security controls, which isolate data in the cloud, have been developed alongside the core infrastructure technology since the system's inception. Security is thus a key component of each of Google's cloud computing elements (e.g., compartmentalization, server assignment, data storage, and processing). Google has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Google has established incident response processes to report and handle events related to confidentiality. Google also establishes agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchange with external parties.

People

Google has implemented a process-based service quality environment designed to deliver the Google Apps, Google Cloud Platform and Other Google Services to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes, the hiring and development of highly skilled resources, and leading industry practices. Google's repeatable process model includes key infrastructure and product related processes controls over security, availability, process integrity, and confidentiality.

Formal organizational structures exist and are available to Google employees on the Company's intranet. The intranet provides drill-down functionality for identifying employees in the operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies and procedures are periodically reviewed and updated as necessary

EXHIBIT D

Google for Education

G Suite for Education (Online) Agreement

This G Suite for Education Agreement (the"**Agreement**") is entered into by and between Google Inc. ("**Google**"), and the customer identified in the Ordering Document ("**Customer**"). This Agreement is effective as of the date Customer clicks the "I Accept" button below or, if applicable, the date the Agreement is countersigned (the "**Effective Date**"). If you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand this Agreement; and (iii) you agree, on behalf of the party that you represent, to this Agreement. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button below (or, if applicable, do not sign this Agreement). This Agreement governs Customer's access to and use of the Services and will be effective as of the Effective Date.

1. Services.

1.1 **Facilities and Data Transfer.** All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

1.2 **Modifications.**

a. **To the Services.** Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such material change.

b. **To URL Terms.** Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Google via the Help Center within thirty days after receiving notice of the change. If Customer notifies Google as required, then Customer will remain governed by the terms in effect immediately prior to the change until the end of the then-current Term. If the Services are renewed, they will be renewed under Google's then current URL Terms.

1.3 **Aliases.** Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

1.4 **Ads.** Google does not serve Ads in the Services or use Customer Data for Ads purposes.

1.5 **End User Accounts.** Customer may request End User Accounts by:(i) requesting them online via the Admin Console; or (ii) after the Services Commencement Date, contacting Google support personnel. Customer can suspend or delete End User Accounts at any point in time through the Admin Console.

1.6 **Google Vault.** If Customer purchases Google Vault, the following additional terms apply:

a. **Retention.** Google will have no obligation to retain any archived Customer Data beyond the retention period specified by Customer (other than for any legal holds). If Customer does not renew Google Vault, Google will have no obligation to retain any archived Customer Data.

b. **Initial Purchase of Google Vault.** At its initial purchase of Google Vault, Customer agrees to purchase Google Vault End User Accounts for all of its Staff who have G Suite for Education End User Accounts. Customer may use Google Vault for Students and Alumni at no charge.

c. **Additional Staff End User Accounts.** After Customer has made its initial purchase of Google Vault, if during any Services Term Customer adds at least 20% more Staff End User Accounts than it purchased previously during that Services Term, Customer agrees to purchase Google Vault for those additional End User Accounts for the remainder of Customer's then current Google Vault Services Term. In addition, on each anniversary of the Billing Start Date, Customer agrees to purchase Google Vault for any additional Staff End User Accounts it adds beyond those purchased previously, for the remainder of Customer's then current Google Vault Services Term.

1.7 **Privacy Notice.** The G Suite for Education Privacy Notice governs how Google collects and uses information from Customer or End Users.

2. Customer Obligations.

2.1 **Permitted Uses.** The Services are permitted for use only by (a) non-profit educational institutions and (b) other non-profit entities (as defined under the relevant state statutes).

2.2 **Compliance.** Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications, features or functionality for the Services available from time to time, the use of which may be contingent upon Customer's agreement to additional terms. In addition, Google will make other Non-G Suite Products (beyond the Services) available to Customer and its End Users in accordance with the Non-G Suite Product Terms and the applicable product-specific Google terms of service. If Customer does not desire to enable any of the Non-G Suite Products, Customer can enable or disable them at any time through the Admin Console.

2.3 **Customer Administration of the Services.** Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

2.4 **End User Consent.** Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

2.5 **Parental Consent.** Under section 10.1 below, Customer is responsible for compliance with the Children's Online Privacy Protection Act of 1998, including obtaining parental consent for collection of personal information in the Services or Non-G Suite Products Customer allows End Users to access. Customer will also obtain parental consent before allowing any End Users under the age of 18 to use Non-G Suite Products.

2.6 **Unauthorized Use.** Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.7 **Restrictions on Use.** Unless Google specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

2.8 **Third Party Requests.** Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.

3. **<u>Payment.</u>** If any of the Services are purchased for a Fee, the terms in this Section 3 apply to those Services.

3.1 **Payment.** All Fees are due thirty days from the invoice date. All payments due are in U.S. dollars unless otherwise indicated in an Order Form. Payments made via wire transfer must include the following instructions:

Bank Name:	ABA Number:	Account Number:
Wells Fargo Bank Palo Alto, California USA	121000248 Google Inc.	4375669785

3.2 **Delinquent Payments.** Delinquent payments may bear interest at the rate of one-and-one-half percent per month (or the highest rate permitted by law, if less) from the payment due date until paid in full. Customer will be responsible for all reasonable expenses (including attorneys' fees) incurred by Google in collecting such delinquent amounts, except where such delinquent amounts are due to Google's billing inaccuracies.

3.3 **Purchase Orders.**

a. **Required.** If Customer wants a Purchase Order number on its invoice, Customer will inform Google and issue a Purchase Order to Google. If Customer requires a Purchase Order, and fails to provide the Purchase Order to Google, then Google will not be obligated to provide the Services until the Purchase Order has been received by Google. Any terms and conditions on a Purchase Order do not apply to this Agreement and are null and void.

b. **Not Required.** If Customer does not require a Purchase Order number to be included on the invoice, Customer will provide Google a waiver of the Purchase Order requirement, which may be an email to this effect. If Customer waives the Purchase Order requirement, then: (a) Google will invoice Customer without a Purchase Order; and (b) Customer agrees to pay invoices without a Purchase Order.

3.4 **Taxes.** Customer is responsible for any Taxes, and Customer will pay Google for the Services without any reduction for Taxes. If Google is obligated to collect or pay Taxes, the Taxes will be invoiced to Customer, unless Customer provides Google with a valid tax exemption certificate authorized by the appropriate taxing authority. If Customer is required by law to withhold any Taxes from its payments to Google, Customer must provide Google with an official tax receipt or other appropriate documentation to support such payments.

3.5 **Invoice Disputes.** Any invoice disputes must be submitted prior to the invoice due date. If the parties determine that certain billing inaccuracies are attributable to Google, Google will not issue a corrected invoice, but will instead issue a credit memo specifying the incorrect amount in the affected invoice. If the disputed invoice has not yet been paid, Google will apply the credit memo amount to the disputed invoice and Customer will be responsible for paying the resulting net balance due on that invoice.

4. **<u>Invoicing; Rates.</u>** If any of the Services are purchased for a Fee, the terms in this Section 4 apply to those Services. On or after the Billing Start Date, Google will invoice Customer the following Fees for each applicable

Service: in advance for the Monthly Charge, Annual Charge or Initial Term Charge (as applicable), all of which will be set forth in the Order Form.

5. **Technical Support Services.**

5.1 **By Customer.** Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Services. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Google.

5.2 **By Google.** If Customer cannot resolve a support issue consistent with the above, then Customer may escalate the issue to Google in accordance with the TSS Guidelines. Google will provide TSS to Customer in accordance with the TSS Guidelines.

6. **Suspension.**

6.1 **Of End User Accounts by Google.** If Google becomes aware of an End User's violation of the Agreement, then Google may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Google's request to Suspend an End User Account, then Google may do so. The duration of any Suspension by Google will be until the applicable End User has cured the breach, which caused the Suspension.

6.2 **Emergency Security Issues.** Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

7. **Confidential Information.**

7.1 **Obligations.** Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.

7.2 **Exceptions.** Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

7.3 **Required Disclosure.** Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

7.4 **FERPA.** The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records"); and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a "School Official" (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.

8. **Intellectual Property Rights; Brand Features.**

8.1 **Intellectual Property Rights.** Except as expressly set forth herein, 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.

8.2 **Display of Brand Features.** Google may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Services) within designated areas of the Services Pages. Customer may specify the nature of this use using the Admin Console. Google may also display Google Brand Features on the Services Pages to indicate that Google provides the Services. Neither party may display or use the other party's Brand Features beyond what is allowed in this Agreement without the other party's prior written consent.

8.3 **Brand Features Limitation.** Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party's right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

9. **Publicity.** Customer agrees that Google may include Customer's name or Brand Features in a list of Google customers, online or in promotional materials. Customer also agrees that Google may verbally reference Customer as a customer of the Google products or services that are the subject of this Agreement. This Section is subject to Section 8.3.

10. **Representations, Warranties and Disclaimers.**

10.1 **Representations and Warranties.** Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA. Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users.

10.2 **Disclaimers.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

11. **Term; Fees.**

11.1 **Agreement Term.** This Agreement will remain in effect for the Term.

11.2 **Services Term and Purchases During Services Term.** Google will provide the Services to Customer during the Services Term. Unless the parties agree otherwise in writing, End User Accounts added during any Services Term will have a prorated term ending on the last day of that Services Term.

11.3 **Auto Renewal.** At the end of each Services Term, the Services (and all End User Accounts previously purchased for a Fee) will automatically renew for an additional Services Term of twelve months. If either party does not want the Services to renew, then it must notify the other party in writing at least 15 days prior to the end of the then current Services Term. This notice of non-renewal will be effective upon the conclusion of the then current Services Term.

11.4 **Fees.** During the Initial Term, Google will not charge Customer Fees for the Services (other than for Google Vault or paid storage, if applicable). Upon the parties' mutual written agreement, (a) Google may charge Customer Fees for the Services after the Initial Services Term and (b) Google may charge Customer

Fees for a premium version of the Services or for optional functionality or enhancements that may be added to the Services by Google (such as Google Vault or paid storage, if applicable).

11.5 **Services Use.** Customer has no obligation to use the Services and may cease using the Services at any time for any reason (or no reason).

11.6 **Revising Rates.** For Services which Customer has purchased for a Fee, Google may revise its rates for the following Services Term by providing Customer written notice (which may be by email) at least thirty days prior to the start of the following Services Term.

12. Termination.

12.1 **Termination for Breach.** Either party may suspend performance or terminate this Agreement if: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.

12.2 **Other Termination.** Customer may terminate this Agreement for any reason (or no reason) with thirty days prior written notice to Google, provided, however, that Customer will remain obligated to pay any Fees for Services which Customer has purchased applicable to the remainder of the then-current Services Term for those Services.

12.3 **Effects of Termination.** If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates, if applicable, for the Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.

13. Indemnification.

13.1 **By Google.** Google will indemnify, defend, and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim that Google's technology used to provide the Services or any Google Brand Feature infringe or misappropriate any patent, copyright, trade secret or trademark of such third party. Notwithstanding the foregoing, in no event shall Google have any obligations or liability under this Section arising from: (i) use of the Services or Google Brand Features in a modified form or in combination with materials not furnished by Google, and (ii) any content, information or data provided by Customer, End Users or other third parties.

13.2 **Possible Infringement.**

(a) **Repair, Replace, or Modify.** If Google reasonably believes the Services infringe a third party's Intellectual Property Rights, then Google will: (a) obtain the right for Customer, at Google's expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe.

(b) **Suspension or Termination.** If Google does not believe the foregoing options are commercially reasonable, then Google may suspend or terminate Customer's use of the impacted Services. If Google terminates the impacted Services, then Google will provide a pro-rata refund of the unearned Fees (if applicable) actually paid by Customer applicable to the period following termination of such Services.

13.3 **General.** Customer will promptly notify Google of the claim and cooperate with Google in defending the claim. Google has full control and authority over the defense, except that: (a) any settlement requiring Customer to admit liability or to pay any money will require Customer's prior written consent, such consent not to be unreasonably withheld or delayed; and (b) Customer may join in the defense with its own counsel at its own expense. THE INDEMNITY ABOVE IS CUSTOMER'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY GOOGLE OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

14. Limitation of Liability.

14.1 **Limitation on Indirect Liability.** NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

14.2 **Limitation on Amount of Liability.** NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE GREATER OF: (I) ONE THOUSAND DOLLARS OR (II) THE AMOUNT PAID BY CUSTOMER TO GOOGLE UNDER THIS AGREEMENT DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

14.3 **Exceptions to Limitations.** These limitations of liability apply to the fullest extent permitted by applicable law, but do not apply to breaches of confidentiality obligations, violations of a party's Intellectual Property Rights by the other party, or indemnification obligations.

15. Miscellaneous.

15.1 **Notices.** Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact; and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

15.2 **Assignment.** Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

15.3 **Change of Control.** Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and thirty days after it receives the written notice in subsection (a).

15.4 **Force Majeure.** Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

15.5 **No Waiver.** Failure to enforce any provision of this Agreement will not constitute a waiver.

15.6 **Severability.** If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.

15.7 **No Agency.** The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

15.8 **No Third-Party Beneficiaries.** There are no third-party beneficiaries to this Agreement.

15.9 **Equitable Relief.** Nothing in this Agreement will limit either party's ability to seek equitable relief.

15.10 **Governing Law.**

a. **For City, County and State Government Entities.** If Customer is a city, county, or state government entity, then the parties agree to remain silent regarding governing law and venue.

b. **For All other Entities.** If Customer is any entity not set forth in Section 15.10(a) then the following applies: This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

15.11 **Amendments.** Any amendment must be in writing and expressly state that it is amending this Agreement.

15.12 **Survival.** The following Sections will survive expiration or termination of this Agreement: 7 (Confidential Information), 8.1 (Intellectual Property Rights), 12.3 (Effects of Termination), 13 (Indemnification), 14 (Limitation of Liability), 15 (Miscellaneous), and 16 (Definitions).

15.13 **Entire Agreement.** This Agreement, and all documents referenced herein, is the parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. If Customer is presented with a similar agreement on the same subject matter upon its log in to use the Services, this Agreement supersedes and replaces that agreement. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.

15.14 **Interpretation of Conflicting Terms.** If there is a conflict between the documents that make up this Agreement, the documents will control in the following order: the Order Form (if applicable), the Agreement, and the terms located at any URL.

15.15 **Counterparts.** The parties may enter into this Agreement by executing the applicable Order Form (if any) or this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

16. **Definitions.**

"**Acceptable Use Policy**" means the acceptable use policy for the Services available at https://www.google.com/apps/intl/en/terms/use_policy.html or such other URL as may be provided by Google.

"**Admin Account(s)**" means the administrative account(s) provided to Customer by Google for the purpose of administering the Services. The use of the Admin Account(s) requires a password, which Google will provide to Customer.

"**Admin Console**" means the online tool provided by Google to Customer for use in reporting and certain other administration functions.

"**Administrators**" mean the Customer-designated technical personnel who administer the Services to End Users on Customer's behalf.

"**Ads**" means online advertisements, excluding advertisements provided by any advertising products that are not part of the Services (for example, Google AdSense) that Customer chooses to use in connection with the Services, displayed by Google to End Users.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

"**Agreement**" means, as applicable either this G Suite for Education Agreement, or the combination of an Order Form and this G Suite for Education Agreement.

"**Alumni**" means graduates or former Students of Customer.

"**Annual Charge**" means the annual charge for the Services set forth in the Order Form (if applicable).

"**Billing Start Date**" means the date upon which Customer will begin paying Google for the Services (if applicable).

"**Brand Features**" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

"**Confidential Information**" means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is considered Customer's Confidential Information.

"**Customer Data**" means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users.

"**Customer Domain Names**" means the domain names owned or controlled by Customer, which will be used in connection with the Services, as identified in the Order Form. Customer may provide the Services to any of its sub-domains (for example, if Customer Domain Name is "edu.com", a sub-domain may include "alumni.edu.com") without written approval from Google.

"**Effective Date**" means the date this Agreement is countersigned.

"**Emergency Security Issue**" means either: (a) Customer's use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other customers' use of the Services; or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

"**End Users**" means the individuals Customer permits to use the Services.

"**End User Account**" means a Google-hosted account established by Customer through the Services for an End User.

"**Export Control Laws**" means all applicable export and re-export control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State.

"**Fees**" means the amounts invoiced to Customer by Google for the Services (if applicable) as described in this Agreement.

"**FERPA**" means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

"**G Suite for Education Privacy Notice**" means the notice at the following URL: https://www.google.com/intl/en/work/apps/terms/education_privacy.html, or such other URL as Google may provide.

"**Help Center**" means the Google help center accessible at https://www.google.com/support/, or other such URL as Google may provide.

"**High Risk Activities**" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

"Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

"Initial Services Term" means the term for the applicable Services beginning on the Service Commencement Date and continuing for the "Current Services Term" set forth in the Order Form from the Billing Start Date (if an Order Form applies to the Services) or if no Order Form applies to the Services, for the term that begins on the Effective Date and continues for one year.

"Initial Term Charge" means the charge for the Services for the Initial Services Term (excluding any applicable one time fees), as set forth in the Order Form (if applicable).

"Monthly Charge" means the monthly charge for the Services set forth in the Order Form (if applicable).

"Non-G Suite Products" means Google products which are not part of the Services, but which may be accessed by End Users using their End User Account login and password. The Non-G Suite Products are set forth at the following URL: https://www.google.com/support/a/bin/answer.py?hl=en&answer=181865, or such other URL as Google may provide.

"Non-G Suite Product Terms" means the terms found at the following URL: https://www.google.com/apps/intl/en/terms/additional_services.html, or such other URL as Google may provide from time to time.

"Notification Email Address" means the email address designated by Customer to receive email notifications from Google. Customer may change this email address through the Admin Console.

"Order Form" means an order form, which is the written document provided by Google specifying the Services Customer will purchase from Google for a Fee (if any) under the Agreement. The Order Form will contain: (i) a signature block for Customer, or for both Customer and Google; (ii) applicable service SKUs; (iii) Fees (if applicable); and (iv) number of, and current Services Term for, any End User Accounts.

"Purchase Order" means a Customer issued purchase order.

"Services" means the G Suite for Education Core Services, Google Classroom, and, if applicable, the Google Vault Services provided by Google and used by Customer under this Agreement. The Services are described here: https://www.google.com/apps/intl/en/terms/user_features.html, or such other URL as Google may provide.

"Service Commencement Date" is the date upon which Google makes the Services available to Customer.

"Services Pages" mean the web pages displaying the Services to End Users.

"Services Term" means the Initial Services Term and all renewal terms for the applicable Services.

"SLA" means the Services Level Agreement located here: https://www.google.com/apps/intl/en/terms/sla.html, or other such URL as Google may provide.

"Staff" means an individual (including any faculty) who is or has been employed by Customer. Any Student or Alumni who are also Staff are deemed Staff under this Agreement (and excluded from the Student or Alumni definition) if they have been employed by Customer within the last twelve months.

"Student" means an individual who has been registered for classes offered by Customer within the last twelve months.

"Suspend" means the immediate disabling of access to the Services, or components of the Services, as applicable, to prevent further use of the Services.

"Taxes" means any duties, customs fees, or taxes (other than Google's income tax) associated with the sale of the Services, including any related penalties or interest.

"Term" means the term of the Agreement, which will begin on the Effective Date and continue until the earlier of: (i) the end of the last Services Term or (ii) the Agreement is terminated as set forth herein.

"Third Party Request" means a request from a third party for records relating to an End User's use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"TSS" means the technical support services provided by Google to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Google's technical support services guidelines then in effect for the Services. TSS Guidelines are at the following URL: https://www.google.com/apps/intl/en/terms/tssg.html or such other URL as Google may provide.

"URL Terms" means the Acceptable Use Policy, the SLA, and the TSS Guidelines.

EXHIBIT E

Google for Education

G Suite for Education Privacy Notice

This Privacy Notice is meant to help G Suite for Education users and parents understand what data we collect, why we collect it, and what we do with it. This Notice summarizes the most relevant portions of the Google Privacy Policy, and includes information about our privacy practices that are specific to Apps for Education. We hope you will take the time to read this Notice and the Google Privacy Policy, which both apply to Apps for Education accounts.

Information we collect

A G Suite for Education account is a Google Account created and managed by a school for use by students and educators. When creating this account, the school may provide Google with certain personal information about its students and educators, including, for example, a user's name, email address, and password. Google may also collect personal information directly from users of G Suite for Education accounts, such as telephone number or a profile photo added to the Apps for Education account.

Google also collects information based on the use of our services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number of the user;
- log information, including details of how a user used our service, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How we use information we collect

In G Suite for Education Core Services

The G Suite for Education Core Services ("Core Services") are Gmail, Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault. These services are provided to a school under its Apps for Education agreement and, as applicable, Data Processing Amendment. (Users and parents can ask their school if it has accepted the Data Processing Amendment.) The Apps for Education agreement as amended applies to the Apps for Education Core Services only.

Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

In Google services generally

The Google Privacy Policy describes fully how Google services generally use information, including for Apps for Education users. To summarize, we use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer users tailored content, such as more relevant search results. We may combine personal information from one service with information, including personal information, from other Google services.

For Apps for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an Apps for Education Account) to target ads, whether in Core Services or other Google services accessed while using an Apps for Education account.

Information users share

A school may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google. Our services provide users with various options for sharing and removing content.

Information we share

Information we collect may be shared outside of Google in limited circumstances. We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With user consent.** We will share personal information with companies, organizations or individuals outside of Google when we have user consent or parents' consent (as applicable).
- **With G Suite for Education administrators.** G Suite for Education administrators have access to information stored in the Google Accounts of users in that school or domain.
- **For external processing.** We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.
- **For legal reasons.** We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
    - meet any applicable law, regulation, legal process or enforceable governmental request.
    - enforce applicable Terms of Service, including investigation of potential violations.
    - detect, prevent, or otherwise address fraud, security or technical issues.
    - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personal information publicly and with our partners – like publishers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

Transparency and choice

We provide a variety of user controls that enable Apps for Education users to make meaningful choices about how information is used in Google services. Depending on the settings enabled by the school, users can use the various controls described in the Privacy Policy, such as Google activity controls, to manage their privacy and information. We provide additional information for parents, students, and administrators on the Apps for Education Privacy Center.

Parental review and deletion of information

The parents of Apps for Education users in Primary/Secondary (K-12) schools can access their child's personal information or request that it be deleted through the school administrator. School administrators can provide for parental access and deletion of personal information consistent with the functionality of our services. If a parent wishes to stop any further collection or use of the child's information, the parent can request that the administrator use the service controls available to them to limit the child's access to features or services, or delete the child's account entirely. Guidance for administrators on how to use service controls to accomplish this is available in the G Suite Help Center.

Interpretation of conflicting terms

This Notice is generally consistent with the Google Privacy Policy and the Apps for Education agreement. Where there are terms that differ, as with the limitations on advertising in Apps for Education, the G Suite for Education agreement (as amended) takes precedence, followed by this Privacy Notice and then the Google Privacy Policy.

Contact us

If you have questions about management of Apps for Education accounts or use of personal information by a school, please contact the Apps for Education account administrator. If you have questions about our practices, please visit the G Suite for Education Privacy Center. Also see our Privacy Troubleshooter for more questions about privacy and Google's products and services. Apps for Education administrators can contact Google about the information in this Notice by submitting the contact form while signed in to their administrator account.

Google

1600 Amphitheatre Parkway, Mountain View, CA 94043 USA

Phone: +1 650-253-0000

EXHIBIT F

Google Apps

- Businesses
- Schools
- Organisations
-
- Applications
- Admin features
- Tours & demos
- Customers
- Apps Marketplace
- FAQ
-
- News & events
- Contact sales
- Support

ADDITIONAL TERMS FOR USE OF ADDITIONAL SERVICES

You are signing up for, or have previously entered into, a Google Apps agreement ("**Google Apps Agreement**") for Services (as defined under the terms of your Google Apps Agreement) between the entity that signs up for (or has agreed to) the Google Apps Agreement ("**the Customer**") and Google Inc., Google Ireland Limited or Google Asia Pacific Pte. Ltd. (as may be applicable, "**Google**"). Google may make more Google applications (beyond the Services) available from time to time through the control panel for the customer domain ("**Additional Services**"). By using such Additional Services, the Customer agrees to the additional terms below ("**Additional Terms**"). If the Customer does not wish to enable any of the Additional Services or you do not have the requisite authority to bind the Customer to these Additional Terms, please disable such Additional Services in the control panel. Capitalised terms used below, but not defined below, have the meaning ascribed to them under the Google Apps Agreement.

1. **Not Subject to your Google Apps Agreement**. The Additional Services are not governed by the Google Apps Agreement, but are governed only by the applicable service-specific Google terms of service. The Additional Services with their respective terms of service are located at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865 (or such other URL that Google may provide).
2. **Existing Customers**. If you are an existing Customer who signed up before 9 November 2010, these Additional Services will be made available by clicking "I ACCEPT" on the confirmation page of the Google Apps transition wizard.
3. **New Customers**. If you are a new Customer who has signed up on or after 9 November 2010, the Additional Services are provided on an "opt-out" basis. The default setting for the Additional Services is on.
4. **Use Constitutes Acceptance**. Use of any Additional Service by any End User constitutes the Customer's acceptance of the Google terms of service for such Additional Service.
5. **Enabling or Disabling Additional Services**. At any point in time, the Customer can enable or disable any of the Additional Services in the control panel.
6. **Future Services**. Google may offer other Additional Services that are not currently set forth at the URL in Section 1 and for which Google does not yet have terms of service. When these future Additional Services become available, they will be offered to the Customer under these Additional Terms.
7. **Availability**. Not all Additional Services may be available in all countries.
8. **Technical Support**. Google will not provide the TSS for the Additional Services. The Customer is responsible for responding to any questions and complaints by End Users relating to the Customer's or its End Users'

use of the Additional Services. Google provides technical support services for the Additional Services solely through the applicable product-specific Help Centre, which is accessible at http://www.google.com/support/ (or such URL that Google may provide).

9. **Third Party Requests**. The Customer is responsible for responding to Third Party Requests that apply to the Additional Services, unless otherwise stated in the applicable terms for each Additional Service. Google does not assist the Customer with responding to such Third Party Requests.
10. **Compliance with Laws**. The Customer is responsible for ensuring that its End Users comply with the applicable Google terms of service for each Additional Service. Where applicable, the Customer agrees that it is solely responsible for compliance with all laws and regulations that apply to the Customer's provision of these Additional Service to the Customer's End Users, such as the U.S. Family Educational Rights and Privacy Act of 1974 (FERPA), Children's Internet Protection Act (CIPA) and the Children's Online Privacy Protection Act of 1998 (COPPA), including but not limited to, obtaining parental consent concerning collection or dissemination of personal information (including that of students) used in connection with the provisioning and use of the Additional Services by the Customer and End Users.
11. **Privacy**. The Customer may have the ability to access, monitor, use or disclose data provided by End Users for these Additional Services or disable an End User's Account for these Additional Services. The Customer will notify End Users of the Customer's ability to take these actions.
12. **Google Checkout**. A Google Checkout account opened by an End User is the End User's personal account and is subject to extensive regulatory requirements and prohibitions. While the Customer may suspend an End User's access to his or her Checkout account, the Customer may not use an End User's Checkout account or make any changes to the information in such Checkout account. The Customer may access information in an End User's Checkout account only in accordance with Checkout privacy policies and the Customer's privacy policy.
13. **Refund for Paid Services**. If the Customer disables an Additional Service for which the Customer or End User has provided payment, Google will not be obligated to refund the Customer or any End User for unused paid services. The Customer will indemnify, defend and hold harmless Google from and against all liabilities, damages, losses and expenses and costs (including settlement costs and reasonable lawyers' fees) arising out of an End User's claim concerning refunds for such paid services.
14. **Google is Data Processor**. Where applicable, the parties agree that Google is a data processor and the Customer is a data controller with respect to the End User personal data contained in the Additional Services for the Customer's domain.
15. **Data Location**. As part of providing the Additional Services, Google may store and process the data provided through such Additional Services

in the United States or any other country in which Google or its agents maintain facilities.

16. **Severability**. If any provision of these Additional Terms is found to be unenforceable, the balance of the Additional Terms will remain in full force and effect.
17. **Modifications**. Google may modify these Additional Terms from time to time.

EXHIBIT G

G Suite

Data Processing Amendment to G Suite Agreement

The Customer agreeing to these terms ("**Customer**") and Google Inc., Google Ireland Limited, Google Commerce Limited or Google Asia Pacific Pte. Ltd. (as applicable, "**Google**") have entered into a G Suite Agreement, G Suite Enterprise Agreement, G Suite Agreement, G Suite via Reseller Agreement, G Suite Enterprise via Reseller Agreement, G Suite via Reseller Agreement, G Suite for Education Agreement or G Suite for Education via Reseller Agreement, as applicable (as amended to date, the "**G Suite Agreement**"). This amendment (the "**Data Processing Amendment**") is entered into by Customer and Google as of the Amendment Effective Date and amends the G Suite Agreement.

The "**Amendment Effective Date**" is: (a) if this Data Processing Amendment is incorporated into the G Suite Agreement by reference, the effective date of the G Suite Agreement, as defined in that agreement; or (b) if this Data Processing Amendment is not incorporated into the G Suite Agreement by reference, the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

If this Data Processing Amendment is not incorporated into the G Suite Agreement by reference and you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms; (ii) you have read and understand these terms; and (iii) you agree, on behalf of the party you represent, to this Data Processing Amendment. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button.

1. **Introduction.**

   This Data Processing Amendment reflects the parties' agreement with respect to terms governing the processing of Customer Data under the G Suite Agreement.

2. **Definitions.**

   2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given in the G Suite Agreement. In this Data Processing Amendment, unless expressly stated otherwise:

   "**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

   "**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any Google Affiliate display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using the "Google Sites" functionality within the Services).

   "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

   "**Agreement**" means the G Suite Agreement, as amended by this Data Processing Amendment and as may be further amended from time to time in accordance with the G Suite Agreement.

   "**Customer Data**" means data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Data Incident**" means (a) any unlawful access to Customer Data stored in the Services or systems, equipment or facilities of Google or its Sub-processors, or (b) unauthorized access to such Services, systems, equipment or facilities that results in loss, disclosure or alteration of Customer Data.

"**Data Privacy Officer**" means Google's Data Privacy Officer for Apps.

"**Data Protection Legislation**" means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**EEA**" means the European Economic Area.

"**Google Group**" means those Google Affiliates involved in provision of the Services to Customer.

"**Instructions**" means Customer's written instructions to Google consisting of the Agreement, including instructions to Google to provide the Services and technical support for the Services as set out in the Agreement; instructions given by Customer, its Affiliates and End Users via the Admin Console and otherwise in its and their use of the Services and related technical support services; and any subsequent written instructions given by Customer to Google and acknowledged by Google.

"**Model Contract Clauses**" or "**MCCs**" means the standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Safe Harbor Certification**" means a current certification to the U.S. Department of Commerce Safe Harbor framework requirements as set out at the following URL: http://export.gov/safeharbor/eu/eg_main_018475.asp, or any replacement framework or URL from time to time.

"**Services**" means, for purposes of this Data Processing Amendment, the G Suite Services which are described at www.google.com/apps/intl/en/terms/user_features.html (as such services and URL link may be updated or modified by Google from time to time in accordance with the G Suite Agreement).

"**Subprocessors**" means (a) all Google Group entities that have logical access to and process Customer Data (each, a "**Google Group Subprocessor**"); and (b) all third parties (other than Google Group entities) that are engaged to provide services to Customer and that have logical access to and process Customer Data (each, a "**Third Party Subprocessor**").

"**Term**" means the term of the G Suite Agreement, as defined in that agreement.

"**Third Party Auditor**" means a qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

2.2. The terms "personal data", "processing", "data subject", "controller" and "processor" have the meanings given to them in the Directive. The terms "data importer" and "data exporter" have the meanings given to them in the

Model Contract Clauses.

3. Term.

This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry or termination of the G Suite Agreement, will remain in effect until, and automatically terminate upon, deletion by Google of all data as described in Section 7 (Data Deletion) of this Data Processing Amendment.

4. Data Protection Legislation.

The parties agree and acknowledge that the Data Protection Legislation may apply to the processing of Customer Data.

5. Processing of Customer Data.

5.1. **Controller and Processor**. If the Data Protection Legislation applies to the processing of Customer Data, then as between the parties, the parties acknowledge and agree that: (a) Customer is the controller of Customer Data under the Agreement; (b) Google is a processor of such data; (c) Customer will comply with its obligations as a controller under the Data Protection Legislation; and (d) Google will comply with its obligations as a processor under the Agreement. If under the Data Protection Legislation a Customer Affiliate is considered the controller (either alone or jointly with the Customer) with respect to certain Customer Data, Customer represents and warrants to Google that Customer is authorized (i) to give the Instructions to Google and otherwise act on behalf of such Customer Affiliate in relation to such Customer Data as described in this Data Processing Amendment, and (ii) to bind the Customer Affiliate to the terms of this Data Processing Amendment.

5.2. **Scope of Processing**. Google will only process Customer Data in accordance with the Instructions, and will not process Customer Data for any other purpose.

5.3. **Processing Restrictions**. Notwithstanding any other term of the Agreement, Google will not process Customer Data for Advertising purposes or serve Advertising in the Services.

5.4. **Additional Products**. Customer acknowledges that if it installs, uses, or enables Additional Products, the Services may allow such Additional Products to access Customer Data as required for the interoperation of those Additional Products with the Services. This Data Processing Amendment does not apply to the processing of data transmitted to or from such Additional Products. Customer can enable or disable Additional Products. Customer is not required to use Additional Products in order to use the Services.

6. Data Security; Security Compliance; Audits.

6.1. **Security Measures**. Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing, as detailed in Appendix 2 ("**Security Measures**"). Google may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. Customer agrees that it is solely responsible for its use of the Services, including securing its account authentication credentials, and that Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (e.g., offline or on-premise storage).

6.2. **Security Compliance by Google Staff**. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

6.3. **Data Incidents**. If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.4. **Compliance with Security and Privacy Standards; SOC 2 and 3 Reports**. During the Term, Google will maintain the following:

(a) its ISO/IEC 27001:2013 Certification or a comparable certification ("**ISO 27001 Certification**") for the Services;

(b) conformity of the Services with ISO/IEC 27018:2014 or a comparable standard ("**ISO 27018 Conformity**"), as independently verified;

(c) its confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability as related to the Services (the "**SOC 2 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months; and

(d) its Service Organization Control (SOC) 3 Report (or a comparable report) as related to the Services (the "**SOC 3 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months.

6.5. **Auditing Security Compliance**

6.5.1. **Reviews of Security Documentation.** Google will make the following available for review by Customer:

(a) the certificate issued in relation to Google's ISO 27001 Certification;

(b) the then-current SOC 3 Report;

(c) a summary or redacted version of the then-current confidential SOC 2 Report; and

(d) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2. **Customer Audits.** If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 of this Data Processing Amendment, Customer or such Customer Affiliate may exercise the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses:

(a) by instructing Google to execute the audit as described in Sections 6.4 and 6.5.1 above; and/or

(b) following a request by Customer in accordance with Section 6.5.4 below, by executing an audit as described in such Model Contract Clauses.

6.5.3. **Additional Business Terms for Reviews and Audits.** Google and Customer (or an authorized Customer Affiliate if applicable) will discuss and agree in advance on:

(a) the reasonable date(s) of and security and confidentiality controls applicable to any Customer review under Section 6.5.1(d); and

(b) the identity of a suitably qualified and independent third party auditor for any audit under Section 6.5.2(b), and the reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit.

Google reserves the right to charge a fee (based on Google's reasonable costs) for any review under Section 6.5.1(d) and/or audit under Section 6.5.2(b). For clarity, Google is not responsible for any costs incurred or fees charged by any third party auditor appointed by Customer (or an authorized Customer Affiliate) in connection with an audit under Section 6.5.2(b). Nothing in this Section 6.5 varies or modifies any rights or obligations of Customer (or any authorized Customer Affiliate) or Google Inc. under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA) of this Data Processing Amendment.

6.5.4. **Requests for Reviews and Audits.** Any requests under Section 6.5.1 or 6.5.2 must be sent to the Data Privacy Officer as described in Section 9 (Data Privacy Officer) of this Data Processing Amendment.

7. **Data Deletion.**

7.1. **Deletion by Customer and End Users**. During the Term, Google will provide Customer or End Users with the ability to delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash" ("**Customer-Deleted Data**"), Google will delete such data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.2. **Deletion on Standard Termination**. On expiry or termination of the G Suite Agreement (or, if applicable, on expiry of any post-termination period during which Google may agree to continue providing the Services), Google will, subject to Section 7.3 (Deletion on Termination for Non-Payment or No Purchase) below, delete all Customer-Deleted Data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.3. **Deletion on Termination for Non-Payment or No Purchase**. On termination of the G Suite Agreement due to Customer breaching its payment obligations or opting not to purchase the Services at the end of a free trial of the Services, Google will delete all Customer Data from its systems within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

8. **Access to Data.**

8.1. **Access; Export of Data**. During the Term, Google will provide Customer with access to and the ability to correct, block and export Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Services during the Term, does not have the ability to correct or block Customer Data as required by applicable law, or to migrate Customer Data to another system or service provider, Google will comply with any reasonable requests by Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

8.2. **End User Requests**. During the Term, if Google receives any request from an End User for records relating to that End User's personal data included in the Customer Data, Google will advise such End User to submit its request to Customer. Customer will be responsible for responding to any such request using the functionality of the Services.

9. **Data Privacy Officer.**

The Data Privacy Officer can be contacted by Customer Administrators at: https://support.google.com/a/contact/gfw_dpo (or via such other means as may be provided by Google). Administrators must be signed in to their Admin Account to use this address.

10. **Data Transfers.**

10.1. **Data Storage and Processing Facilities**. Google may store and process Customer Data in the United States or any other country in which Google or any of its Subprocessors maintains facilities, subject to Section 10.2 (Transfers of Data Out of the EEA) below.

10.2. **Transfers of Data Out of the EEA**. If the storage and processing of Customer Data (as set out in Section 10.1 above) involves transfers of Customer personal data out of the EEA and Data Protection Legislation applies to those transfers, Google will:

10.2.1 ensure that Google Inc. maintains its Safe Harbor Certification, and that the transfers are made in accordance with such Safe Harbor Certification; and/or

10.2.2 ensure that Google Inc. as the data importer of such Customer personal data enters into Model Contract Clauses with Customer (or an authorized Customer Affiliate) as the data exporter of such data, if Customer so requests, and that the transfers are made in accordance with any such Model Contract Clauses; and/or

10.2.3 adopt an alternative solution that achieves compliance with the terms of the Directive for transfers of personal data to a third country, and ensure that the transfers are made in accordance with any such compliance solution.

10.3. **Safe Harbor Certification and Processing Practices**. While Google Inc. maintains its Safe Harbor Certification pursuant to Section 10.2.1, Google will ensure that: (a) the scope of such Safe Harbor Certification includes Customer Data; and (b) the Google Group's processing practices in respect of Customer Data remain consistent with those described in such Safe Harbor Certification.

10.4. **Data Center Information**. Google will make available to Customer information about the countries in which data centers used to store Customer Data are located.

11. **Subprocessors.**

11.1. **Subprocessors**. Google may engage Subprocessors to provide parts of the Services and related technical support services, subject to the restrictions in this Data Processing Amendment.

11.2. **Subprocessing Restrictions**. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required by the following, as applicable pursuant to Section 10.2 (Transfers of Data Out of the EEA): (a) any Safe Harbor Certification maintained by Google Inc.; (b) any Model Contract Clauses entered into by Google Inc. and Customer (or an authorized Customer Affiliate); and/or (c) any alternative compliance solution adopted by Google.

11.3. **Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the Agreement. If the Model Contract Clauses have been entered into as described above, Customer (or, if applicable, an authorized Customer Affiliate) consents to Google Inc. subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses.

11.4. **Additional Information**. Information about Third Party Subprocessors is available at the following URL: www.google.com/intl/en/work/apps/terms/subprocessors.html, as such URL may be updated by Google from time to time. The information available at the URL is accurate at the time of publication. At the written request of the Customer, Google will provide additional information regarding Subprocessors and their locations. Any such requests must be sent to the Data Privacy Officer for G Suite as described in Section 9 (Data Privacy Officer) of this Data Processing Amendment.

11.5. **Termination**. Google will, at least 15 days before appointing any new Third Party Subprocessor, inform Customer of the appointment (including the name and location of such subprocessor and the activities it will perform) either by sending an email to the Notification Email Address or via the Admin Console. If Customer objects to Google's use of any new Third Party Subprocessor, Customer may, as its sole and exclusive remedy, terminate the G Suite Agreement by giving written notice to Google within 30 days of being informed by Google of the appointment of such subprocessor.

12. **Liability Cap.**

If Google Inc. and Customer (or an authorized Customer Affiliate) enter into Model Contract Clauses as described above, then, subject to the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability), the total combined liability of Google and its Affiliates, on the one hand, and Customer and its Affiliates, on the other hand, under or in connection with the Agreement and all those MCCs combined will be limited to the maximum monetary or payment-based liability amount set out in the Agreement.

13. **Third Party Beneficiary.**

Notwithstanding anything to the contrary in the Agreement, where Google Inc. is not a party to the Agreement, Google Inc. will be a third party beneficiary of Section 6.5 (Auditing Security Compliance), Section 11.3 (Consent to Subprocessing) and Section 12 (Liability Cap) of this Data Processing Amendment.

14. **Effect of Amendment.**

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, the Agreement remains in full force and effect.

Appendix 1: Categories of Data and Data Subjects

Categories of Data

Personal data submitted, stored, sent or received by Customer or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other electronic data

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As of the Amendment Effective Date, Google will take and implement the Security Measures set out in this Appendix to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. **Data Center & 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, and 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 diesel generator systems take over. The diesel 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 replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) **Networks & 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.

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 End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

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 personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal 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. LDAP, Kerberos and a proprietary system utilizing RSA keys 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 password expiry, 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 & Authentication**.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and 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). A central authentication system is used across all Services to increase uniform security of data.

The 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 End Users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) **Decommissioned Disks and Disk Erase Policy**.

Certain 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 (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. **Subprocessor Security.**

Prior to 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 always to the requirements set out in Section 11.2 (Subprocessing Restrictions) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

G Suite Data Processing Amendment, Version 1.5

EXHIBIT H

Google for Education

Privacy & Security Information

The mission of Google is to organize the world's infc

That is why we provide educators with powerful solutions that are affordable and easy t

Find answers to frequently asked questions

G Suite for Education core services

C

A

Google for Education

G Suite for Education (formerly called Google Apps for Education)

The G Suite for Education (formerly called Google Apps for Education) core services are

Schools can use G Suite core services in compliance with COPPA and FERPA. G Suite cc

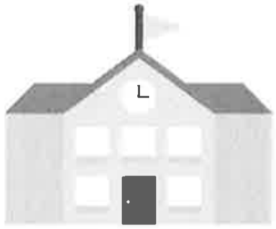
More than 50 million students, teachers and administrators in almost every country in th

Please note that there are additional services outside of the G Suite core services that G

Google for Education

READ OUR G SUITE PRIVACY NOTICE

READ OUR G SUITE AGREEMENT (GOOGLE'S CONTRACT WITH SCHOOLS COVERING G SUITE CORE SERVICES)



Does Google own school or student data?

No. Google doesn't assume ownership of any customer data in G Suite core services, and it says so in our contracts (under "Intellectual Property").

We provide powerful, easy-to-use management tools and dashboards to help administrators keep track of their organization's services, usage and data. We only keep your personal information as long as you ask us to keep it. If an education department, school or university decides to stop using Google, we make it easy for them to take their data with them.

READ THE CONTRACT (SECTION ON "INTELLECTUAL PROPERTY")

Google for Education

Does Google sell school data to third parties?

No. We don't sell your G Suite data to third parties, and we do not share personal information placed in our systems with third parties, except in the few exceptional circumstances described in the G Suite agreement and our Privacy Policy, such as when you ask us to share it or when we are required to do so by law.

MORE ABOUT INFORMATION SHARING ▶

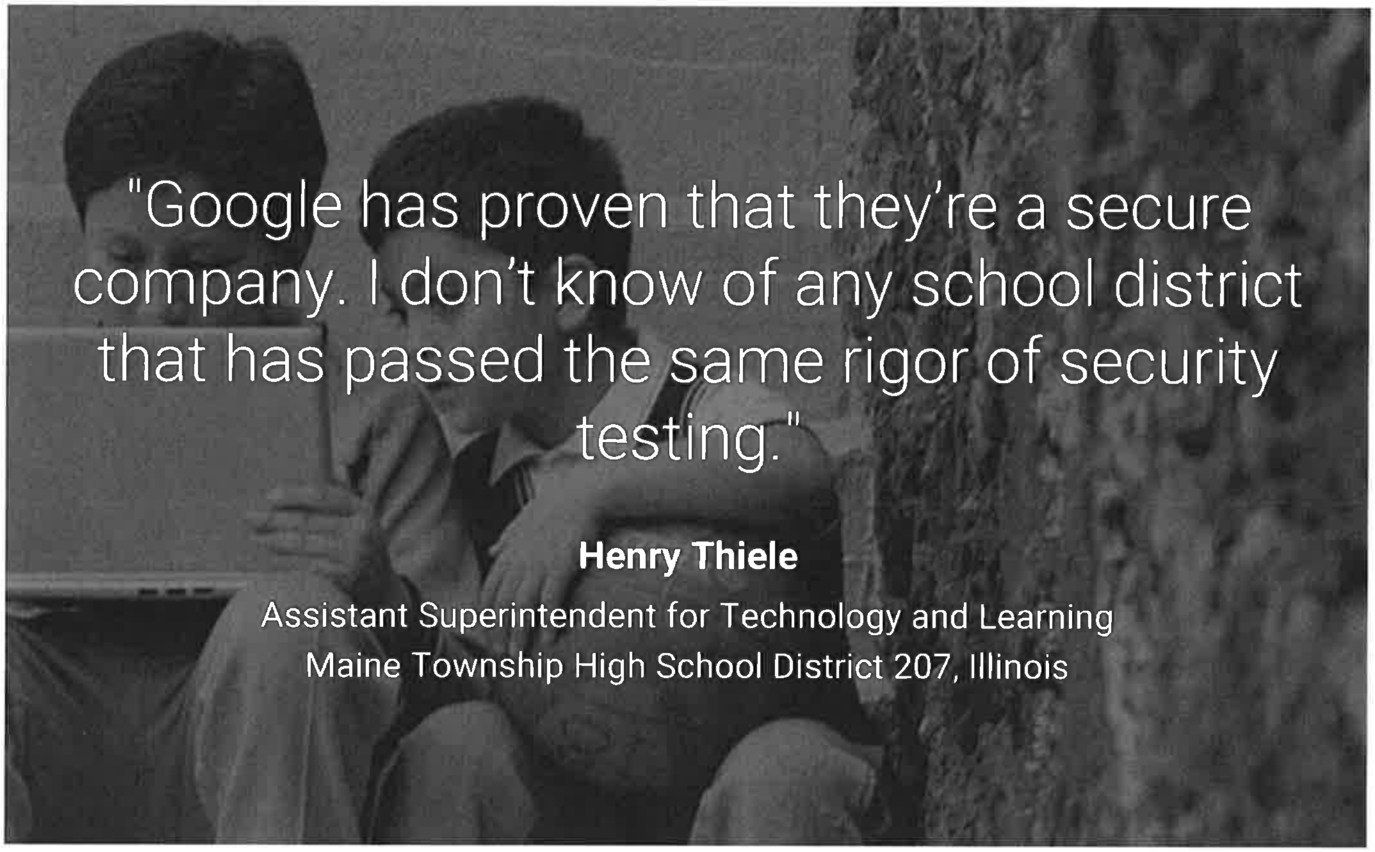
Are there ads in G Suite?

No. There are no ads in the suite of G Suite core services. Outside of the G Suite Core Services, additional Google services may show ads, as described in the G Suite Privacy Notice. For G Suite users in Primary/Secondary (K-12) schools, Google does not use any user personal information (or any information associated with a Google Account) to target ads.

READ OUR G SUITE AGREEMENT (GOOGLE'S CONTRACT WITH SCHOOLS COVERING G SUITE CORE SERVICES) ▶

MORE ABOUT PRIVACY ▶

Google for Education



"Google has proven that they're a secure company. I don't know of any school district that has passed the same rigor of security testing."

Henry Thiele

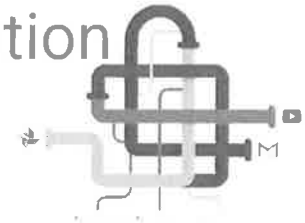
Assistant Superintendent for Technology and Learning
Maine Township High School District 207, Illinois

How does Google keep data secure?

We are fully committed to the security and privacy of your data and protecting you and your school from attempts to compromise it. Our systems are among the industry's most secure and we vigorously resist any unlawful attempt to access our customers' data.

MORE ABOUT SECURITY ▶

Google for Education



How does Google ensure its tools are reliable?

Our proven infrastructure handles more than 100 billion search queries each month and scales services such as Gmail to hundreds of millions of users with 99.978% availability and no scheduled downtime. We have more than 450 full-time engineers, the world's foremost experts in security, working to protect your information.

MORE ABOUT RELIABILITY ▶

Which third parties have reviewed Google's security practices?

We connect with independent auditors to review our data protection practices. Ernst & Young, an independent auditor, has verified that our practices and contractual commitments for G Suite comply with ISO/IEC 27018:2014. G Suite and our data centers are also SSAE 16 / ISAE 3402 Type II SOC 2-audited and have achieved ISO 27001 certification.

MORE ABOUT COMPLIANCE ▶

DETAILS OF SOC3 ▶

Google for Educati

How do you know we’re keeping our word?

We make contractual commitments in our G Suite agreement and commit to comply with privacy and security standards here. And whether it’s real time dashboards to verify system performance, our ongoing auditing of our processes or sharing the location of our datacenters, we’re committed to providing all our users utmost transparency. It’s your data, and we want you to know what happens with it so that you can always make informed choices.

Has Google signed the Student Privacy Pledge?

Yes. In order to to reaffirm the commitments we've made to schools, Google has signed the Student Privacy Pledge. This pledge, introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA), is intended to reflect our commitment to safeguard student personal information in our services designed for use in schools.

STUDENT PRIVACY PLEDGE SIGNATORY

Google for Education

What kind of scanning or indexing of user data is done on G Suite for Education accounts?

G Suite services don't collect or use student data for advertising purposes or to create ads profiles.

Gmail for consumers and G Suite users runs on the same infrastructure, which helps us deliver high performance, reliability, and security to all of our users. However, G Suite is a separate offering that provides additional security, administrative and archiving controls for education, work and government customers.

Like many email providers, we do scanning in Gmail to keep our customers secure and to improve their product experience. In Gmail for G Suite, this includes virus and spam protection, spell check, relevant search results and features like Priority Inbox and auto-detection of calendar events. Scanning to provide product features is done on all incoming emails and is 100% automated. We do NOT scan G Suite emails for advertising purposes.

Google for Education

Can G Suite for Education be used in compliance with the Family Educational Rights and Privacy Act (FERPA)?

Yes. G Suite core services comply with the Family Educational Rights and Privacy Act (FERPA) and our commitment to do so is included in our agreements.

LEARN MORE ABOUT FERPA ▶

Given changes around the U.S.-E.U. Safe Harbor Agreement, what options does G Suite for Education offer for meeting E.U. Data Protection Directive requirements?

Schools can opt into our data processing amendment and model contract clauses. These are an additional means of meeting the adequacy and security requirements of the E.U. Data Protection Directive. Model contract clauses were created specifically by the European Commission to permit the transfer of personal data from Europe.

If you have not already done so, we'd like to remind our G Suite customers to consider opting-in to the data-processing amendment and model contract clauses.

SEE OPT-IN INSTRUCTIONS ▶

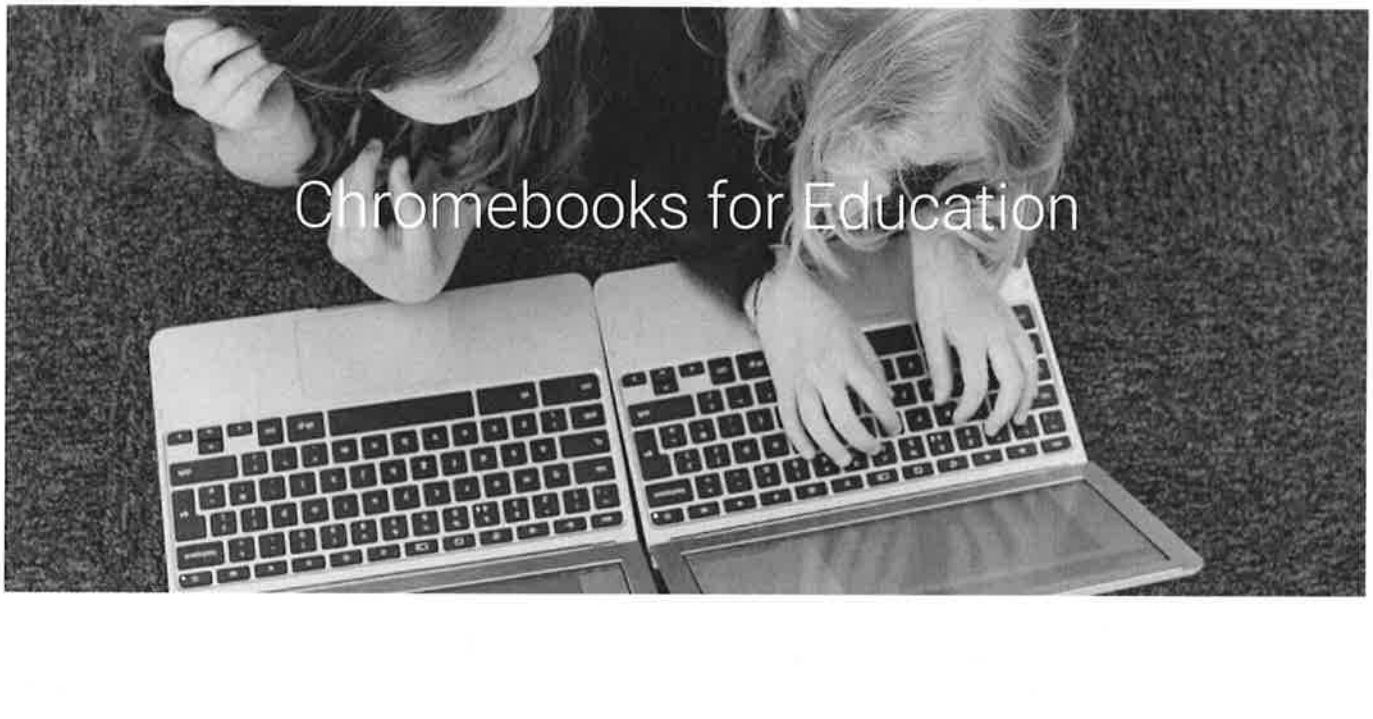
MORE ABOUT MODEL CONTRACT CLAUSES ▶

Can G Suite for Education be used in compliance with the Children's Online Privacy Protection Act of 1998 (COPPA)?

Yes. We contractually require that schools using G Suite get the parental consent required by COPPA. Our services can be used in compliance with COPPA as long as a school has parental consent.

READ COPPA ▶

READ OUR HELP CENTER ARTICLE "GETTING CONSENT FOR G SUITE" ▶



Chromebooks for Education

Google for Education

Millions of students use Chromebooks for learning. Privacy and security features helped

Although Chromebooks are not a core service, we ensure they comply with the Student

Are Chromebooks secure for my students?

Yes. Chromebooks are designed with multiple layers of security to keep them safe from viruses and malware without any additional security software. A full 10% of boot time is dedicated to re-verifying that the device has not been tampered with, so every time you power on a Chromebook, your security is checked. And because they can be managed from the web, Chromebooks make it easy for school administrators to configure policies and settings, like enabling safe browsing or blocking malicious sites.

MORE ABOUT CHROMEBOOK SECURITY ▶

MORE ABOUT CHROMEBOOK PRIVACY ▶

READ THE CHROME PRIVACY WHITEPAPER ▶

Google for Education

Are Chromebooks compatible with online testing?

Chromebooks are a secure platform for administering student assessments, and when setup properly, these devices meet K-12 education testing standards. With Chromebooks, you can disable students' access to browse the web during an exam in addition to disabling external storage, screenshots, and the ability to print. Both PARCC (see TestNav) and the Smarter Balanced Assessment consortia have verified that Chromebooks meet hardware and operating system requirements for online student.

How is data used and protected for students on Chromebooks for Education?

Chrome Sync enables Google Account holders to log into any Chromebook or Chrome browser and find all their apps, extensions, bookmarks and frequently visited web pages. For students, this means that they can get to work right away. That's one of the reasons Chromebooks have become so popular in classrooms, especially for schools that can't afford a device for every child. With Chromebooks and Chrome Sync, students can have a personalized experience on any device they share with their classmates.

Personally-identifiable Chrome Sync data in G Suite accounts is only used to power features in Chrome for that person, for example allowing students to access their own browsing data and settings, securely, across devices. In addition, our systems compile data aggregated from millions of users of Chrome Sync and, after completely removing information about individual users, we use this data to holistically improve the services we provide. For example if data shows that millions of people are visiting a webpage that is broken, that site would be moved lower in the search results. This is not connected to any specific person nor is it used to analyze student behaviors. If they choose to, administrators can disable Chrome Sync and users can choose what information to sync. G Suite users' Chrome Sync data is not used to target ads to individual students.

Google for Education

Schools can control whether students or teachers can use additional Google consumer

Most Additional Services are governed by the Google Terms of Service and Privacy Poli

We allow school leaders to decide whether to turn these services on or off for certain gr

LEARN MORE ABOUT G SUITE CORE AND ADDITIONAL SERVICES

LEARN MORE ABOUT ADDITIONAL SERVICES THAT CAN BE USED WITH G SUITE ACCOUNTS, AND SEE ANY SERV

READ THE GOOGLE TERMS OF SERVICE

READ THE GOOGLE PRIVACY POLICY THAT GOVERNS MANY ADDITIONAL SERVICES

How can families keep their kids safe online?

Along with this page, which provides detail on the services we offer to schools, you can find guidance for keeping your kids safe online outside of school. We worked with many partners to create the Google Family Safety Center.

VISIT THE GOOGLE FAMILY SAFETY CENTER

Where can I get more details?

Google for Education

READ OUR G SUITE AGREEMENT (GOOGLE'S CONTRACT WITH SCHOOLS COVERING G SUITE CORE SERVICES)

EXHIBIT I

Google

Privacy Policy

Last modified: June 28, 2016 (view archived versions) (The hyperlinked examples are available at the end of this document.)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you **more relevant search results** and ads, to help you **connect with people** or to make **sharing with others quicker and easier**. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which **ads you'll find most useful**, **the people who matter most to you online**, or which YouTube videos you might like.

We collect information in the following ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or **credit card** to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

- **Information we get from your use of our services.** We **collect information** about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or **view and interact with our ads** and content. This information includes:

  - **Device information**

    We collect **device-specific information** (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your **device identifiers** or **phone number** with your Google Account.

  - **Log information**

    When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

    - details of how you used our service, such as your search queries.
    - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
    - Internet protocol address.

    - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
    - cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use Google services, we **may collect and process information about your actual location**. We use various technologies to determine location, including IP address, GPS, **and other sensors** that may, for example, provide Google with information on nearby devices, **Wi-Fi access points and cell towers**.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and similar technologies**

  We **and our partners** use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as **advertising services** or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is **linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites**.

Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information. For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.

How we use information we collect

We use the information we collect from all of our services to **provide, maintain**, **protect** and improve them, to **develop new ones**, and to **protect Google and our users**. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to **limit sharing or visibility settings** in your Google Account.

When you contact Google, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to **improve your user experience** and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

We may **combine personal information from one service with information, including personal information, from other Google services** – for example **to make it easier to share things with people you know**. Depending on your account settings, **your activity on other sites and apps** may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services. You can also visit these controls to manage whether certain activity is stored in a cookie or similar technology on your device when you use our services while signed-out of your account.
- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your preferences about the Google ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also opt out of certain Google advertising services here.
- Adjust how the Profile associated with your Google Account appears to others.
- Control who you share information with through your Google Account.
- Take information associated with your Google Account out of many of our services.
- Choose whether your Profile name and Profile photo appear in shared endorsements that appear in ads.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services **may not function properly** if your cookies are disabled. For example, we may not remember your language preferences.

Information you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on **sharing** and **removing your content**.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with **access to your personal information**. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup systems).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, **legal process or enforceable governmental request**.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

  We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation, **legal process or enforceable governmental request**.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent, or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly **to show trends** about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

When this Privacy Policy applies

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including YouTube, services Google provides on

Android devices, and services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Compliance and cooperation with regulatory authorities

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

- Chrome and Chrome OS
- Play Books
- Payments
- Fiber
- Project Fi
- Google Apps for Education

For more information about some of our most popular services, you can visit the Google Product Privacy Guide.

Other useful privacy and security related materials

Further useful privacy and security related materials can be found through Google's policies and principles pages, including:

- Information about our technologies and principles, which includes, among other things, more information on
  - how Google uses cookies.
  - technologies we use for advertising.
  - how we recognize patterns like faces.
- A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.
- The Privacy Checkup tool, which makes it easy to review your key privacy settings.
- Google's safety center, which provides information on how to stay safe and secure online.

"access to your personal information"

For example, with Google Dashboard you can quickly and easily see some of the data associated with your Google Account. Learn more.

"ads you'll find most useful"

For example, if you frequently visit websites and blogs about gardening, you may see ads related to gardening as you browse the web. Learn more.

"advertising services"

For example, if you frequently visit websites and blogs about gardening that show our ads, you may start to see ads related to this interest as you browse the web.
Learn more.

"and other sensors"

Your device may have sensors that provide information to assist in a better understanding of your location. For example, an accelerometer can be used to determine things like speed, or a gyroscope to figure out direction of travel.
Learn more.

"collect information"

This includes information like your usage data and preferences, Gmail messages, G+ profile, photos, videos, browsing history, map searches, docs, or other Google-hosted content.
Learn more.

"combine personal information from one service with information, including personal information, from other Google services"

For example, when you're signed in to your Google Account and search on Google, you can see search results from the public web, along with pages, photos, and Google+ posts from your friends and people who know you or follow you on Google+ may see your posts and profile in their results.
Learn more.

"connect with people"

For example, you could get suggestions of people you might know or want to connect with on Google+, based on the connections you have with people on other Google products, like Gmail and people who have a connection with you may see your profile as a suggestion.
Learn more.

"credit card"

Whilst we currently don't ask for a credit card during sign up, verifying your age through a small credit card transaction is one way to confirm that you meet our age requirements in case your account was disabled after you have entered a birthday indicating you are not old enough to have a Google Account.
Learn more.

"develop new ones"

For example, Google's spell checking software was developed by analyzing previous searches where users had corrected their own spelling.
Learn more.

"device identifiers"

Device identifiers let Google know which unique device you are using to access our services, which can be used to customise our service to your device or analyse any device issues related to our services.
Learn more.

"device-specific information"

For example, when you visit Google Play from your desktop, Google can use this information to help you decide on which devices you'd like your purchases to be available for use.
Learn more.

"improve your user experience"

For example, cookies allow us to analyse how users interact with our services.
Learn more.

"legal process or enforceable governmental request"

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to hand over user data. Our legal team reviews each and every request, regardless of type, and we frequently push back when the requests appear to be overly broad or don't follow the correct process.
Learn more.

"limit sharing or visibility settings"

For example, you can choose your settings so your name and photo do not appear in an ad.
Learn more.

"linked with information about visits to multiple sites"

Google Analytics is based on first-party cookies. Data generated through Google Analytics can be linked, by the Google Analytics customer or by Google, using Google technology, to third-party cookies, related to visits to other websites, for instance when an advertiser wants to use its Google Analytics data to create more relevant ads, or to further analyze its traffic.
Learn more.

"maintain"

For example, we continuously monitor our systems to check that they are working as intended and in order to detect and fix errors.
Learn more.

"may collect and process information about your actual location"

For example, Google Maps can center the maps view on your current location.
Learn more.

"may not function properly"

For example, we use a cookie called 'lbcs' which makes it possible for you to open many Google Docs in one browser.
Learn more.

"and our partners"

We allow trusted businesses to use cookies or similar technologies for advertising and research purposes on our services.
Learn more.

"phone number"

For example, if you add a phone number as a recovery option, if you forget your password Google can send you a text message with a code to enable you to reset it.
Learn more.

"protect Google and our users"

For example, if you're concerned about unauthorized access to your email, "Last account activity" in Gmail shows you information about recent activity in your email, such as the IP addresses that accessed your mail, the associated location, as well as the time and date.
Learn more.

"protect"

For example, one reason we collect and analyze IP addresses and cookies is to protect our services against automated abuse.
Learn more.

"provide"

For example, the IP address assigned to your device is used to send the data you requested back to your device.
Learn more.

"sharing"

For example, with Google+, you have many different sharing options.
Learn more.

"sharing with others quicker and easier"

For example, if someone is already a contact, Google will autocomplete their name if you want to add them to a message in Gmail.
Learn more.

"the people who matter most to you online"

For example, when you type an address in the To, Cc, or Bcc field of a message you're composing, Gmail will suggest addresses from your Contacts list.
Learn more.

"to make it easier to share things with people you know"

For example, if you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name.
Learn more.

"view and interact with our ads"

For example, we regularly report to advertisers on whether we served their ad to a page and whether that ad was likely to be seen by users (as opposed to, for example, being on part of the page to which users did not scroll).
Learn more.

"We may share aggregated, non-personally identifiable information publicly"

When lots of people start searching for something, it can provide very useful information about particular trends at that time.
Learn more.

"Wi-Fi access points and cell towers"

For example, Google can approximate your device's location based on the known location of nearby cell towers.
Learn more.

"more relevant search results"

For example, we can make search more relevant and interesting for you by including photos, posts, and more from you and your friends.
Learn more.

"removing your content"

For example, you can delete your Web & App Actvity, your blog, a Google Site you own, your YouTube Channel, your Google+ profile or your entire Google account.
Learn more.

"to show trends"

You can see some of these at Google Trends and YouTube Trends.
Learn more.

"your activity on other sites and apps"

This activity might come from your use of Google products like Chrome Sync or from your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics). These products share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.
Learn more.

EXHIBIT J

Google for Work Security and Compliance Whitepaper

How Google protects your data.

Google for Work

This whitepaper applies to the following Google Apps products

Google Apps for Work, Education, Government, Nonprofit, Drive for Work, and Google Apps Unlimited

Table of Contents

Introduction

Cloud computing offers many advantages and conveniences for today's organizations. Employees can work together in documents in real time from their phone or tablet from any location, and communicate instantly with teammates via video, voice, instant message, or email. No longer tied to a single machine, they have the freedom to work together from anywhere, using any device they choose. Meanwhile, their employers don't shoulder the cost or burden of maintaining servers and constantly updating software. It's no surprise, then, that so many organizations around the world are storing their information and getting work done in the cloud.

The growth of the cloud has thrust the issue of security and trust into the spotlight. That's because cloud services operate very differently from traditional on-premises technology. Rather than residing on local servers, content is now managed on Google servers that are part of our global data center network. In the past, organizations felt that they had complete control over how infrastructure was run and who operated it. Organizations moving to the cloud will rely on cloud suppliers to manage the infrastructure, operations, and delivery of services. In this new world, companies will still control company data, but via cloud-based tools and dashboards. Rather than only using desktop computers, users can now access work files on their personal mobile devices. Customers must assess whether the security controls and compliance of any cloud solution meet their individual requirements. Customers must therefore understand how these solutions protect and process their data. The goal of this whitepaper is to provide an introduction to Google's technology in the context of security and compliance.

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than many traditional on-premises solutions. We make security a priority to protect our own operations, but because Google runs on the same infrastructure that we make available to our customers, your organization can directly benefit from these protections. That's why we focus on security, and protection of data is among our primary design criteria. Security drives our organizational structure, training priorities and hiring processes. It shapes our data centers and the technology they house. It's central to our everyday operations and disaster planning, including how we address threats. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers.

This paper outlines Google's approach to security and compliance for Google Apps, our cloud-based productivity suite. Used by more than five million organizations worldwide, from large banks and retailers with hundreds of thousands of people to fast-growing startups, Google Apps for Work and Education includes Gmail, Calendar, Groups, Drive, Docs, Sheets, Slides, Hangouts, Sites, Talk, Contacts and Vault. Google Apps is designed to help teams work together in new, more efficient ways, no matter where members are located or what device they happen to be using.

This whitepaper will be divided into two main sections: security and compliance. The security section will include details on organizational and technical controls regarding how Google protects your data. The second section on compliance will cover how your data is processed and details on how organizations can meet regulatory requirements.

Google Has a Strong Security Culture

Google has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Employee background checks

Before they join our staff, Google will verify an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Security training for all employees

All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

Internal security and privacy events

Google hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. One example is "Privacy Week," during which Google hosts events across global offices to raise awareness of privacy in all facets, from software development, data handling and policy enforcement to living our privacy principles. Google also hosts regular "Tech Talks" focusing on subjects that often include security and privacy.

Our dedicated security team

Google employs more than 500 full-time security and privacy professionals, who are part of our software engineering and operations division.
Our team includes some of the world's foremost experts in information, application and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. Google's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Google employs more than 500 full-time security and privacy professionals, who are part of our software engineering and operations division. Our team includes some of the world's foremost experts in information, application and network security.

Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams.
They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

The security team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Some examples of this research would be the discovery of the POODLE SSL 3.0 exploit and cipher suite weaknesses. The security team also publishes security research papers, available to the public. The security team also organizes and participates in open-source projects and academic conferences.

Our dedicated privacy team

The Google Privacy team operates independently from product development and security organizations, but participates in every Google product launch. The team reviews design documentation and code audits to ensure that privacy requirements are followed. The Privacy team has built a set of automated monitoring tools to help ensure that products with Customer Data operate as designed and in accordance with our privacy policy. They help release products that reflect strong privacy standards: transparent collection of user data and providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform. After products launch, the privacy team oversees automated processes that audit data traffic to verify appropriate data usage. In addition, the privacy team conducts research providing thought leadership on privacy best practices for our emerging technologies.

Internal audit and compliance specialists

Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties.

Collaboration with the security research community

Google has long enjoyed a close relationship with the security research community, and we greatly value their help identifying vulnerabilities in Google Apps and other Google products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk, offering rewards in the tens of thousands of dollars. In Chrome, for instance, we warn users against malware and phishing, and offer rewards for finding security bugs. Due to our collaboration with the research community, we've squashed more than 700 Chrome security bugs and have rewarded more than $1.25 million — more than $2 million has been awarded across Google's various vulnerability rewards programs. We publicly thank these individuals and list them as contributors to our products and services.

Operational Security

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

Vulnerability management

Google administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open-source tools. More information about reporting security issues can be found at Google Application Security.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Google takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Google helps tens of millions of people every day to protect themselves from harm by showing warnings to users of Google Chrome, Mozilla Firefox and Apple Safari when they attempt to navigate to websites that would steal their personal information or install software designed to take over their computers. Malware sites or email attachments install malicious software on users' machines to steal private information, perform identity theft, or attack other computers. When people visit these sites, software that takes over their computer is downloaded without their knowledge. Google's malware strategy begins with infection prevention by using manual and automated scanners to scour Google's search index for websites that may be vehicles for malware or phishing. Approximately one billion people use Google's Safe Browsing on a regular basis. Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. In addition to our Safe Browsing solution, Google operates VirusTotal, a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. VirusTotal's mission is to help in improving the antivirus and security industry and make the Internet a safer place through the development of free tools and services.

Google helps tens of millions of people every day to protect themselves from harm by showing warnings to users of Google Chrome, Mozilla Firefox and Apple Safari when they attempt to navigate to websites that would steal their personal information or install software designed to take over their computers.

Google makes use of multiple antivirus engines in Gmail, Drive, servers and workstations to help identify malware that may be missed by antivirus signatures.

Monitoring

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

Incident management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team.

Technology with Security at Its Core

Google Apps runs on a technology platform that is conceived, designed and built to operate securely. Google is an innovator in hardware, software, network and system management technologies. We custom-designed our servers, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

State-of-the-art data centers

Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multifactor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever step foot in one of our data centers.

Powering our data centers

To keep things running 24/7 and ensure uninterrupted services, Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Environmental impact

Google reduces environmental impact of running our data centers by designing and building our own facilities. We install smart temperature controls, use "free-cooling" techniques like using outside air or reused water for cooling, and redesign how power is distributed to reduce unnecessary energy loss. To gauge improvements, we calculate the performance of each facility using comprehensive efficiency measurements. We're the first major Internet services company to gain external certification of our high environmental, workplace safety and energy management standards throughout our data centers. Specifically, we received voluntary ISO 14001, OHSAS 18001 and ISO 50001 certifications. In a nutshell, these standards are built around a very simple concept: Say what you're going to do, then do what you say—and then keep improving.

Custom server hardware and software

Google's data centers house energy-efficient custom, purpose-built servers and network equipment that we design and manufacture ourselves. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Our production servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state.
These automated, self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network.

Hardware tracking and disposal

Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

A global network with unique security benefits

Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe.

In other cloud services and on-premises solutions, customer data must make several journeys between devices, known as "hops," across the public Internet. The number of hops depends on the distance between the customer's ISP and the solution's data center. Each additional hop introduces a new opportunity for data to be attacked or intercepted. Because it's linked to most ISPs in the world, Google's global network improves the security of data in transit by limiting hops across the public Internet.

Defense in depth describes the multiple layers of defense that protect Google's network from external attacks. Only authorized services and protocols that meet our security requirements are allowed to traverse it; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed through custom GFE (Google Front End) servers to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to authorized personnel.

Google's IP data network consists of our own fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services across the globe.

Securing data in transit

Data is most vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Google. Data traveling between a customer's device and Google is encrypted using HTTPS/TLS (Transport Layer Security). In fact, Google was the first major cloud provider to enable HTTPS/TLS by default. When sending to or receiving email from a non-Google user, all links of the chain (device, browser, provider of the email service) have to be strong and work together to make encryption work. We believe this is so important that we report on the industry's adoption of TLS on our safe email site. Google has also upgraded all our RSA certificates to 2048-bit keys, making our encryption in transit for Google Apps and all other Google services even stronger.

Perfect forward secrecy (PFS) minimizes the impact of a compromised key, or a cryptographic breakthrough. It protects network data by using a short-term key that lasts only a couple of days and is only held in memory, rather than a key that's used for years and kept on durable storage. Google was the first major web player to enable perfect forward secrecy by default.

Google encrypts all Google Apps data as it moves between our data centers on our private network.

> Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages.

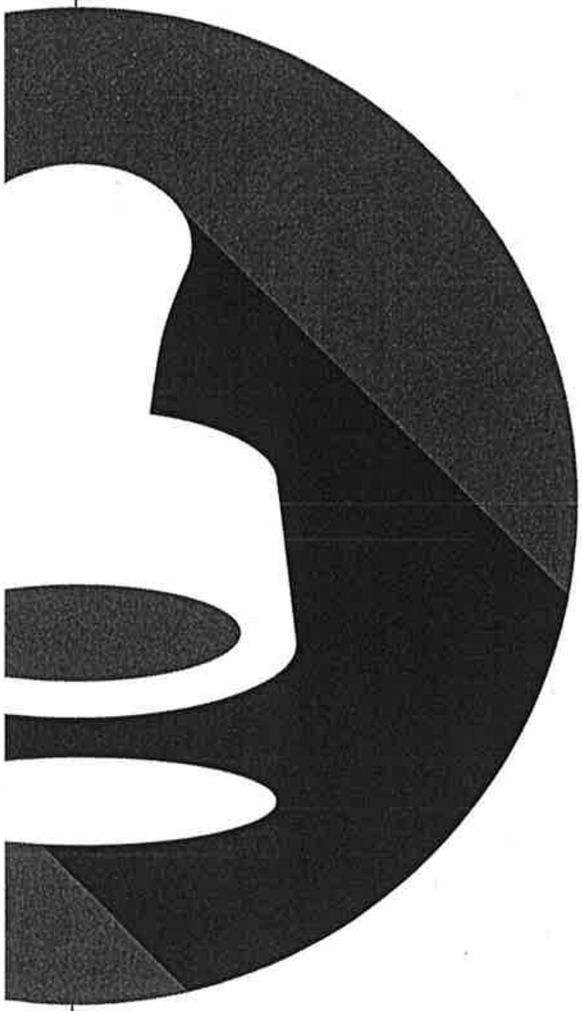
Low latency and highly available solution

Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Apps customers can continue working in most cases without interruption. Customers with global workforces can collaborate on documents, video conferencing and more without additional configuration or expense. Global teams share a highly performant and low latency experience as they work together on a single global network.

Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Apps, our recovery point objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication:

actions you take in Google Apps Products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customer data is divided into digital pieces with random file names. Neither their content nor their file names are stored in readily human-readable format, and stored customer data cannot be traced to a particular customer or application just by inspecting it in storage. Each piece is then replicated in near-real time over multiple disks, multiple servers, and multiple data centers to avoid a single point of failure. To further prepare for the worst, we conduct disaster recovery drills in which we assume that individual data centers—including our corporate headquarters—won't be available for 30 days. We regularly test our readiness for plausible scenarios as well as more imaginative crises, like alien and zombie invasions.

Our highly redundant design has allowed Google to achieve an uptime of 99.984% for Gmail for the last years with **no scheduled downtime**. Simply put, when Google needs to service or upgrade our platform, users do not experience downtime or maintenance windows.



Service availability

Some of Google's services may not be available in some jurisdictions. Often these interruptions are temporary due to network outages, but others are permanent due to government-mandated blocks. Google's Transparency Report also shows recent and ongoing disruptions of traffic to Google products. We provide this data to help the public analyze and understand the availability of online information.

Independent Third-Party Certifications

Google's customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines our data centers, infrastructure, and operations. Regular audits are conducted to certify our compliance with the auditing standards ISO 27001, SOC 2 and SOC 3, as well as with the U.S. Federal Information Security Modernization Act of 2014 (FISMA) for Google Apps for Government. When customers consider Google Apps, these certifications can help them confirm that the product suite meets their security, compliance and data processing needs.

ISO 27001

ISO 27001 is one of the most widely recognized and accepted independent security standards. Google has earned it for the systems, technology, processes, and data centers that run Google Apps. Our compliance with the international standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council (a member of the International Accreditation Forum, or IAF). Our ISO 27001 certificate and scoping document are available in our Trust Center.

SOC 2/3

In 2014, the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) released the revised version of the Trust Services Principles and Criteria (TSP). SOC (Service Organization Controls) is an audit framework for non-privacy principles that include security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports. Our SOC 3 report is available for download without a nondisclosure agreement. The SOC 3 confirms our compliance with the principles of security, availability, processing integrity and confidentiality.

FISMA

FISMA is a U.S. federal law pertaining to the information security of federal agencies' information systems. The law requires agencies to ensure that their systems and those operated by service providers such as Google meet minimum security requirements specified by the National Institute of Standards and Technology (NIST). Google, as a cloud provider, has one of the longest track records in meeting these requirements, and we maintain a current authorization to operate (ATO) for Google Apps for Government. The Federal Risk and Authorization Management Program (FedRAMP) adds a number of requirements on top of the FISMA requirements that cloud providers must meet. For more information on the FedRAMP program and vendor status, please visit fedramp.gov.

Data Usage

Our philosophy

Google Apps customers own their data, not Google. The data that Google Apps organizations and users put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customer administrators to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google.

No advertising in Google Apps

There is **no** advertising in the Google Apps Core Services, and we have no plans to change this in the future. Google does not collect, scan or use data in Google Apps Core Services for advertising purposes. Customer administrators can restrict access to Non-Core Services from the Google Apps Admin console. Google indexes customer data to provide beneficial services, such as spam filtering, virus detection, spellcheck and the ability to search for emails and files within an individual account.

Data Access and Restrictions

Administrative access

To keep data private and secure, Google logically isolates each customer's Google Apps data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Apps products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams.

For customer administrators

Within customer organizations, administrative roles and privileges for Google Apps are configured and controlled by the customer. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data. Integrated audit logs offer a detailed history of administrative actions, helping customers monitor internal access to data and adherence to their own policies.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests; however, like other technology and communications companies, Google may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations. Respect for the privacy and security of data you store with Google remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to comply, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it, and we push back often and when necessary. For example, in 2006 Google was the only major search company that refused a U.S. government request to hand over two months of user search queries. We objected to the subpoena, and eventually a court denied the government's request. In some cases we receive a request for all information associated with a Google account, and we may ask the requesting agency to limit it to a specific product or service. We believe the public deserves to know the full extent to which governments request user information from Google. That's why we became the first company to start regularly publishing reports about government data requests. Detailed information about data requests and Google's response to them is available in our Transparency Report. It is Google's policy to notify customers about requests for their data unless specifically prohibited by law or court order.

We believe the public deserves to know the full extent to which governments request user information from Google. That's why we became the first company to start regularly publishing reports about government data requests.

Third-party suppliers

Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Google Apps, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers

to ensure they 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 third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Regulatory Compliance

Our customers have varying regulatory compliance needs. Our clients operate across regulated industries, including finance, pharmaceutical and manufacturing.

Google contractually commits to the following:

- Google will maintain adherence to ISO 27001 and SOC 2/3 audits during the term of the agreement.
- Defined Security Standards. Google will define how data is processed, stored, and protected through specific defined security standards.
- Access to our Data Privacy Officer. Customers may contact Google's Data Privacy Officer for questions or comments.
- Data Portability. Administrators can export customer data in standard formats at any time during the term of the agreement. Google does not charge a fee for exporting data.

Data processing amendment

Google takes a global approach to our commitments on data processing. Google and many of our customers operate in a global environment. We offer **all** of our users the same high level of protections via our data processing amendment. The commitments in our data processing amendment are designed to facilitate compliance with jurisdictional-specific laws or regulations. Your organization can opt into our data processing amendment by following the instructions in our Help Center.

EU Data Protection Directive

The Article 29 Working Party is an independent European advisory body focused on data protection and privacy. They have provided guidance on how to meet European data privacy requirements when engaging with cloud computing providers. Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party.

U.S.-EU and U.S.-Swiss Safe Harbor Frameworks

More than half of Google's business customers are based outside of the United States, with many of them operating in Europe. These businesses must comply with the European Commission's Data Protection Directive, which regulates the transfer of personal data within the European Union. The U.S.-EU Safe Harbor Framework provides a method for European companies to transfer personal data outside the European Union in a manner that's consistent with the Directive. Google certifies that it adheres to its principles and to those of the U.S.-Swiss Safe Harbor Framework.

EU model contract clauses

In 2010, the European Commission approved model contract clauses as a means of compliance with the requirements of the Directive. The effect of this decision is that by incorporating certain provisions into a contract, personal data can flow from those subject to the Directive to providers outside the EU or the European Economic Area. Google has a broad customer base in Europe. By adopting EU model contract clauses, we're offering customers an additional option for compliance with the Directive.

U.S. Health Insurance Portability and Accountability Act (HIPAA)

Google Apps supports our customers' compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA), which governs the confidentiality and privacy of protected health information (PHI). Customers who are subject to HIPAA and wish to use Google Apps with PHI must sign a business associate agreement (BAA) with Google. The BAA covers Gmail, Google Calendar, Google Drive, Google Sites and Google Apps Vault.

U.S. Family Educational Rights and Privacy Act (FERPA)

More than 30 million students rely on Google Apps for Education. Google Apps for Education services comply with FERPA (Family Educational Rights and Privacy Act) and our commitment to do so is included in our agreements.

Children's Online Privacy Protection Act of 1998 (COPPA)

Protecting children online is important to us. We contractually require Google Apps for Education schools to obtain parental consent that COPPA calls for to use our services, and our services can be used in compliance with COPPA.

Empowering Users and Administrators to Improve Security and Compliance

Google builds security into its structure, technology, operations and approach to customer data. Our robust security infrastructure and systems become the default for each and every Google Apps customer. But beyond these levels, users are actively empowered to enhance and customize their individual security settings to meet their business needs through dashboards and account security wizards. Google Apps also offers administrators full control to configure infrastructure, applications and system integrations in a single dashboard via our Admin console — regardless of the size of the organization. This approach simplifies administration and configuration. Consider deployment of DKIM (a phishing prevention feature) in an on-premise email system. Administrators would need to patch and configure every server separately, and any misconfiguration would cause a service outage. Using our Admin console, DKIM is configured in minutes across thousands or hundreds of thousands of accounts with peace of mind and no outage or maintenance window required. Administrators have many powerful tools at their disposal, such as authentication features like 2-step verification and single sign-on, and email security policies like secure transport (TLS) enforcement, which can be configured by organizations to meet security and system integration requirements. Below are some key features that can help customize Google Apps for your security and compliance needs:

User authentication/authorization features

2-step verification

2-step verification adds an extra layer of security to Google Apps accounts by requiring users to enter a verification code in addition to their username and password when they sign in. This can greatly reduce the risk of unauthorized access if a user's password is compromised. Verification codes are delivered on a one-time basis to a user's Android, BlackBerry, iPhone, or other mobile phone. Administrators can choose to turn on 2-step verification for their domain at any time.

Security Key

Security Key is an enhancement for 2-step verification. Google, working with the FIDO Alliance standards organization, developed the Security Key — an actual physical key used to access your Google Account. It sends an encrypted signature rather than a code, and helps ensure that your login cannot be phished. Google for Work admins will be able to easily deploy, monitor and manage the Security Key at scale with new controls in the Admin console with no additional software to install. IT admins will see where and when employees last used their keys with usage tracking and reports. If Security Keys are lost, admins can easily revoke access to those keys and provide backup codes so employees can still sign-in and get work done.

Single sign-on (SAML 2.0)

Google Apps offers customers a single sign-on (SSO) service that lets users access multiple services using the same sign-in page and authentication credentials. It is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm. Customer organizations can use the SSO service to integrate single sign-on for Google Apps into their LDAP or other SSO system.

OAuth 2.0 and OpenID Connect

Google Apps supports OAuth 2.0 and OpenID Connect, an open protocol for authentication and authorization. This allows customers to configure one single sign-on service (SSO) for multiple cloud solutions. Users can log on to third-party applications through Google Apps—and vice versa—without re-entering their credentials or sharing sensitive password information.

Google Apps also offers administrators full control to configure infrastructure, applications and system integrations in a single dashboard via our Admin console — regardless of the size of the organization.

Data management features

Information Rights Management (IRM)

With Information Rights Management ("IRM") you can disable downloading, printing and copying from the advanced sharing menu -- perfect for when the file you're sharing is only meant for a few select people. This new option is available for any file stored in Google Drive, including documents, spreadsheets and presentations created in Google Docs.

Drive audit log

The **Drive audit log** lists every time your domain's users view, create, update, delete or share Drive content. This includes content you create in Google Docs, Sheets, Slides and other Google Apps, as well as content created elsewhere that you upload to Drive, such as PDFs and Word files.

Drive content compliance / alerting

Google Apps for Work has an additional feature that allows Administrators to keep track of when specific actions are taken in Drive and can set up custom Drive alerts. So if you want to know when a file containing the word "confidential" in the title is shared outside the company, now you'll know. And there are more events coming to Drive audit, including download, print and preview alerts.

Trusted domains for Drive sharing

Google Apps for Work and Education administrators will allow for domain whitelisting. End users can share to those trusted domains, but can't share to other external domains. Great for partnerships, subsidiaries or other arrangements where certain domains are trusted and users are allowed to share to them.

Email Security features

Secure transport (TLS) enforcement

Google Apps administrators can require that email to or from specific domains or email addresses be encrypted with Transport Layer Security (TLS). For instance, a customer organization may choose to transmit all messages to its outside legal counsel via a secure connection. If TLS is not available at a specified domain, inbound mail will be rejected and outbound mail will not be transmitted.

Phishing prevention

Spammers can sometimes forge the "From" address on an email message so that it appears to come from a reputable organization's domain. Known as phishing, this practice is often an attempt to collect sensitive data. To help prevent phishing, Google participates in the DMARC program, which lets domain owners tell email providers how to handle unauthenticated messages from their domain. Google Apps customers can implement DMARC by creating a DMARC record within their admin settings and implementing an SPF record and DKIM keys on all outbound mail streams.

Email content compliance

Administrators can choose to scan Google Apps email messages for predefined sets of words, phrases, text patterns or numerical patterns. They can create rules that either reject matching emails before they reach their intended recipients or deliver them with modifications. Customers have used this setting to monitor sensitive or restricted data, such as credit card information, internal project code names, URLs, telephone numbers, employee identification numbers, and social security numbers.

Google Apps administrators can require that email to or from specific domains or email addresses be encrypted with Transport Layer Security (TLS).

Objectionable content

The objectionable content setting enables administrators to specify what action to perform for messages based on custom word lists. With objectionable content policies, administrators choose whether messages containing certain words (such as obscenities) are rejected or delivered with modifications; for example, to notify others when the content of a message matches the rules that you set. Administrators can also configure this setting to reject outbound emails that may contain sensitive company information; for example, by setting up an outbound filter for the word *confidential*.

Restricted email delivery

By default, users with Gmail accounts at your domain can send mail to and receive mail from any email address. However, in some cases, administrators may want to restrict the email addresses your users can exchange mail with. For example, a school might want to allow its students to exchange mail with the faculty and other students, but not with people outside of the school. Use the Restrict delivery setting to allow the sending or receiving of email messages only from addresses or domains that administrators specify. When administrators add a Restrict delivery setting, users cannot communicate with anyone, except those authorized. Users who attempt to send mail to a domain not listed will see a message that specifies a policy prohibiting mail to that address, confirming that the mail is unsent. Users receive only authenticated messages from listed domains. Messages sent from unlisted domains—or messages from listed domains that can't be verified using DKIM or SPF records—are returned to the sender with a message about the policy.

eDiscovery features

eDiscovery allows organizations to stay prepared in case of lawsuits and other legal matters. Google Vault is the eDiscovery solution for Google Apps that lets customers retain, archive, search and export their business Gmail. Administrators can also search and export files stored in Google Drive.

Email retention policy

Retention rules control how long certain messages in your domain are retained before they are removed from user mailboxes and expunged from all Google systems. Google Apps allows you to set a default retention rule for your entire domain. For more advanced implementations, Google Vault allows administrators to create custom retention rules to retain specific content. This advanced configuration allows administrators to specify the number of days to retain messages, whether to delete them permanently after their retention periods, whether to retain messages with specific labels, and whether to let users manage email deletion themselves.

Legal holds

Google Vault allows administrators to place legal holds on users to preserve all their emails and on-the-record chats indefinitely in order to meet legal or other retention obligations. You can place legal holds on all content in a user's account, or target specific content based on dates and terms. If a user deletes messages that are on hold, the messages are removed from the user's view, but they are not deleted from Google servers until the hold is removed.

Search/discovery

Google Vault allows administrators to search Gmail and Drive accounts by user account, organizational unit, date or keyword. Search results include email, on-the-record chats, Google file types and non-Google file types such as PDF, DOCX and JPG.

Evidence export

Google Vault allows administrators to have the ability to export specific email, on-the-record chats and files to standard formats for additional processing and review in a manner that supports legal matters while respecting chain of custody guidelines.

Support for third-party email platforms

The comprehensive mail storage setting ensures that a copy of all sent or received mail in your domain—including mail sent or received by non-Gmail mailboxes—is stored in the associated users' Gmail mailboxes. For organizations that reroute mail to non-Gmail mail servers, this setting also ensures storage of mail in Gmail mailboxes for archiving and eDiscovery purposes.

Securing endpoints

Mobile device management (MDM)

Mobile device management in Google Apps eliminates the need for on-premises device or third-party management solutions. Administrators can enforce policies over mobile devices in their organization, encrypt data on devices, and perform actions like remotely wiping or locking lost or stolen devices. This type of control helps ensure the security of business data, even if employees choose to work on their personal phones and tablets. Mobile device management in Google Apps works with Android, iOS, Windows Phone, and smartphones and tablets using Microsoft Exchange ActiveSync, such as BlackBerry 10.

Administrators can enforce policies over mobile devices in their organization, encrypt data on devices, and perform actions like remotely wiping or locking lost or stolen devices.

Policy-based Chrome browser security

All of the tools and features in Google Apps are best supported by Google Chrome. **Administrators can apply security and usage policies across Windows, OSX, Linux, iOS, and Android.**
Chrome's standard security features include Safe Browsing, sandboxing, and managed updates that protect users from malicious sites, viruses, malware, and phishing attacks. There are also measures in place to prevent cross-site scripting, which attackers can use to steal private data. Google Apps administrators can deploy Chrome for Work across their organization and customize it to meet their needs.
Over 280 policies help administrators control how employees use Chrome across devices. For example, administrators can enable automatic updates to get the latest security fixes, block or allow specific apps, and configure support for legacy browsers.

Chrome device management

The Google Apps Admin Console applies policy to Chrome devices such as Chromebooks, Chromeboxes, and Chromebox for meetings, which are fast, secure, and cost-effective computers that run Chrome as an operating system. Administrators can easily manage security and other settings for their organization's Chrome devices from a single place. They can configure Chrome features for their users, set up access to VPNs and WiFi networks, pre-install apps and extensions, restrict sign-in to certain users, and more.

Data Recovery

Restore a recently deleted user

An administrator can restore a deleted user account for up to five days after date of deletion. After five days, the Admin console permanently deletes the user account, and it can't be restored, even if you contact Google technical support. Please note that only customer Administrators can delete accounts.

Restore a user's Drive or Gmail data

An administrator can restore a user's Drive or Gmail data for up to 25 days after the data is removed from the user's trash. Google will delete all Customer-deleted data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

An administrator can restore a user's Drive or Gmail data for up to 25 days after date of deletion.

Security reports

Google Apps administrators have access to security reports that provide vital information on their organization's exposure to data compromise. They can quickly discover which particular users pose security risks by eschewing 2-step verification, installing external apps, or sharing documents indiscriminately. Administrators can also choose to receive alerts when suspicious login activity occurs, indicating a possible security threat.

Conclusion

The protection of user data is a primary design consideration for all of Google's infrastructure, applications and personnel operations. Protection of user data is far from being an afterthought or the focus of occasional initiatives, it's an integral part of what we do. We believe that Google can offer a level of protection that very few can match. Because protecting your data is part of our core business, Google can develop security innovations such as 2-step authentication and stronger encryption methods. We are able to make extensive investments in security, resources and expertise at a scale that few can afford. Our scale of operations and collaboration with the security research community enable Google to address vulnerabilities quickly or prevent them entirely. Google's security and operational procedures are verified by independent third-party auditors.

Data protection is more than just security. Google's strong contractual commitments make sure our customers maintain control over the data and how it is processed, including the assurance that your data is not used for advertising or any other purpose than to deliver Google Apps services.

For these reasons and more, over five million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in our platform to allow our users to benefit from our services in a secure and transparent manner.

Data protection is more than just security. Google's strong contractual commitments make sure our customers maintain control over the data and how it is processed, including the assurance that your data is not used for advertising or any other purpose than to deliver Google Apps services.