Google Apps for Education (GAFE) Data Privacy

Data privacy and information security is of great importance to Oak Park Unified School District and we share your concern that student data is handled appropriately and not shared with outside sources without our permission and that all student data remains under our control. We have designed our implementation of cloud based data storage to be as similar as possible to the data access and security we currently have with district hosted files and student files/data on district servers. In addition to Google Apps for Education (GAFE), we will be making use of services from Backupify (www.backupify.com) and Cloudlock (www.cloudlock.com) to ensure that we have an independent archive of all Google Apps For Education data (information stored in Google Drive and Google Email accounts) and the ability to search and monitor the contents of student data stores that is separate from Google and allows us to have a historical record of any data stored within Google accounts, just as we currently do with district hosted file servers that currently hold student files. We have also employed the services of AmplifiedIT (www.amplifiedit.com), the leading K-12 Google Apps for Education consultancy to assist us in configuring out GAFE implementation to ensure that there is no leakage of data or gaps in misconfigurations of the Google Admin console that would lead to a potential security breach or loss of privacy or data. The following are Google's data handling policies downloaded 5/5/2015 from https://www.google.com/edu/trust/

OVERVIEW

No ads in Google Apps for Education services. Period.

There are no ads in Google Apps for Education services and we have no plans to change this in the future. Additionally, K-12 Google Apps for Education users do not see ads when they use Google Search and are signed in to their Apps for Education accounts.

Data ownership and management

Google Apps for Education users own their data, not Google. The data that schools put into our systems is theirs, and we believe it should stay that way—it says so in our contracts.

- We provide powerful, easy-to-use management tools, and dashboards help administrators keep track of their organization's services, usage and data.
- We only keep your data as long as schools require us to keep it.

If an education department, school or university decides to no longer use Google we make it easy for them to take their data with them.

We protect your data

We don't sell your Google Apps for Education 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 your Google Apps agreement and our Privacy Policy, such as when you ask us to share it or when we are required to do so by law.

Family Safety Center

In addition to this page, which provides detail on the security of our services to schools, you can find guidance and tips for keeping families safe online in our Family Safety Center

GOOGLE (GAFE) DATA HANDLING POLICIES

Downloaded 5/5/2015 from https://support.google.com/work/answer/6056650

Privacy

We do everything in our power to protect you and your businesses, schools, and government organizations from attempts to compromise your data. We vigorously resist any unlawful attempt to access our customers' data, whether it be from a hacker or a government body.

In order to help answer some of the many questions we receive, we have created this FAQ and a corresponding Google Apps security site. We hope this helps to answer some of your questions about Google's position on these important issues! Be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

Is Google using my data? What for?

Google processes your data to fulfill our contractual obligation to deliver our services. Google's customers own their data, not Google. The data that companies, schools and students put into our systems is theirs. Google does not sell your data to third parties. Google offers our customers a detailed Data Processing Amendment that describes our commitment to protecting your data.

Does Google use my organization's data in Google Apps services or Cloud Platform for advertising purposes?

No. There are no ads in Google Apps Services or Google Cloud Platform, and we have no plans to change this in the future. We do not scan for advertising purposes in Gmail or other Google Apps services. Google does not collect or use data in Google Apps services for advertising purposes. The situation is different for our free offerings and the consumer space. For information on our free consumer products, be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

Does Google use my organization's data in Google Apps for Education for advertising purposes?

Google Apps for Education services do not collect or use student data for advertising purposes or create advertising profiles.

Gmail for consumers and Google Apps for Education users runs on the same infrastructure, which helps us deliver high performance, reliability and security to all of our users. However, Google Apps is a separate offering that provides additional security, administrative and archiving controls for education, business 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 Google Apps for Education, 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 Google Apps for Education emails for advertising purposes.

Additionally, we do not collect or use any information stored in Apps for Education users' Google Drive or Docs (or Sheets, Slides, Drawings, Forms) for any advertising purposes.

Users who have chosen to show Adsense ads on their Google Sites will still have the ability to display those existing ads on their websites. However, it will no longer be possible to edit or add new AdSense ads to existing sites or to new pages.

What kind of data scanning or indexing of end-user data is done?

Google for Work does not scan your data or email in Google Apps Services for advertising purposes. Our automated systems scan and index your data to provide you with your services and to protect your data, such as to perform spam and malware detection, to sort email for features like Priority Inbox and to return fast, powerful search results when users search for information in their accounts. The situation is different for our free offerings and the consumer space. For information on our free consumer products, be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

Do we maintain ownership of the data we place in Google Apps?

The data that companies, schools and students put into our systems is theirs, whether it's corporate intellectual property, personal information or a homework assignment.

If my company decides to leave Google will we be able to take our data with us?

We provide tools so that you can take your data with you if you choose to use external services in conjunction with Google Apps or stop using our services altogether, without penalty or additional cost imposed by Google.

Does giving Google access to my data create a security risk? How does Google ensure that its employees do not pose a threat?

Google's security practices are verified and certified by third-party auditors. We have achieved ISO 27001 certification, which means that an independent auditor has examined the controls present in our data centers, infrastructure and operation. This certification sets a bar for security that is often higher than what is achieved by many of our customers. Amongst these practices, employees are subject to background investigations based on their level of access. Any employee access is governed by a policy of "least privilege access". This means that access is only granted to the information and resources that are necessary for the execution of the assigned task.

Google may only access data in your account in strict compliance with our Privacy Policy and your Customer Agreement. We also offer a detailed Data Processing Amendment that further describes our commitment to protecting your data.

How can we delete data from Google without leaving footprints? How long will Google keep my organization's data?

We believe that you should have control over your data. When you agree to our Data Processing Amendment, Google contractually commits to deleting your Google Apps data from our systems within 180 days of your deleting it in our Apps services.

Why does it take a maximum of 180 days for my data to be deleted from your systems?
When you delete data, the pointers to that data are removed immediately, but Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine—or even an entire data center—fails, your data will still be accessible. As a result it can take up to 180 days to ensure that every bit of customer data is purged from our systems.

What process do you follow if a third party, such as law enforcement, wants to access my data?
Respect for the privacy and security of the data you store with Google underpins our approach to complying with legal requests for user data. Our legal team reviews each and every government request for user data to make sure it satisfies legal requirements and Google's policies, and we push back when the requests are overly broad or don't follow the correct process.

How do you protect my information from government access?
We push back when government requests are overly broad or don't follow the correct process. We do this frequently, like when we persuaded a court to drastically limit a U.S. government request for two months of user search queries. When we are legally required to comply with these requests, we deliver that information to the authorities. We want you to know that storing your data in a particular country does not necessarily protect the data from access by foreign governments.

Google notifies users about legal demands when appropriate, unless prohibited by law or court order, and since 2009 has published aggregate statistics about government requests for user information in our Transparency Report . Google has been public in its advocacy for increased transparency of these requests. In fact, Google received the highest rating from the Electronic Freedom Frontier (EFF) in their annual Who Has Your Back report on how cloud providers protect data from governmental requests.

Security

We've spent years developing one of the world's most advanced and secure infrastructures. More than 450 full-time engineers—including some of the world's foremost experts in computer security—work to protect your information. Security is at the core of our architecture, and we improve it every day. The Google security team has published hundreds of academic research papers on security. It has led the way in discovering new threats and implementing protections like 2-step verification driving the adoption of encryption.

In order to help answer some of the many questions we receive, we have created this FAQ and a corresponding Google Apps security site. We hope this helps to answer some of your questions about Google's position on these important issues! Be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

How does Google protect against hackers, hacktivists, governments and other intruders?
The technology, scale and agility of our infrastructure bring you unique security benefits. Our data centers are built with custom-designed servers, running our own operating system for

security and performance. Google's 450 security engineers, including some of the world's foremost experts, work around the clock to spot threats early and respond quickly. We get better as we learn from each incident, and even incentivize the security research community, with which we actively engage, to expose our systems' vulnerabilities. Here are a few examples of how security and reliability are at the core of what we do:

- Google's data centers use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimized for security and performance. Since Google controls the entire hardware stack, we are able to quickly respond to any threats or weaknesses that may emerge.

- Google is the first major cloud provider to enable perfect forward secrecy , which encrypts content as it moves between our servers and those of other companies. Many industry peers have followed suit or have committed to adopting it in the future.

- Google encrypts GMail, Attachment, and Drive data while on the move. This ensures that your messages are safe not only when they move between you and Google's servers, but also as they move between Google's data centers.

- To protect against cryptanalytic advances, in 2013, Google doubled the length of our RSA encryption keys to 2048 bits . We change the keys every few weeks, raising the bar for the rest of the industry.

How do I know that others customers sharing the same servers can't access my data?
Your data is logically protected as if it were on its own server. Unauthorized parties cannot access your data. Your competitors cannot access your data, and you can't access theirs. In fact, all user accounts are protected by this secure architecture that ensures that one user cannot see another user's data. This is similar to how customer data is segmented in other shared infrastructures, such as online banking applications.

How do we know you do what you say?
Google Apps and Google Cloud Platform are certified for SSAE 16/ISAE 3402 Type II, received the SOC2 audit and the ISO 27001 certification. This means that an independent auditor has examined the controls protecting the data in Google Apps (including logical security, privacy and data center security) and assured that these controls are in place and operating effectively.

Does Google let others test its security controls? Can our organization conduct our own penetration tests on Google?
Yes. Google values the cutting-edge external contributions that can help keep our users safe, so we maintain a Vulnerability Reward Program for Google-owned web properties. Your organization can sign up for this program. Google was the first major cloud provider to offer a program of this type. More information about this program can be found at http://www.google.com.au/about/appsecurity/reward-program/

Does Google encrypt my data?
Yes. Data is encrypted at several levels. Google forces HTTPS (Hypertext Transfer Protocol

Secure) for all transmissions between users and Google Apps services and uses Perfect Forward Secrecy (PFS) for all its services. Google also encrypts message transmissions with other mail servers using 256-bit Transport Layer Security (TLS) and utilizes 2048 RSA encryption keys for the validation and key exchange phases. This protects message communications when client users send and receive emails with external parties also using TLS.
Perfect Forward Secrecy (PFS) requires that the private keys for a connection are not kept in persistent storage. Anyone who breaks a single key can no longer decrypt months' worth of connections; in fact, not even the server operator is able to retroactively decrypt HTTPS sessions.

Google is constantly working to extend and strengthen encryption across more services and links.

Google Apps includes mobile device management (MDM) for Android and iOS which supports features such as device activation, remote data wipe and policy-based encryption. MDM puts you in control and makes it easy to let your users use their own devices to access corporate information without compromising on security.

Reliability

We make the performance, scale and reliability of Google's technology available to businesses, schools and government institutions. We have built one of the world's most proven infrastructure. It supports more than 100 billion Google searches each month and more than 100 hours of YouTube video uploads each minute. It delivers Gmail and other services to hundreds of millions of users with 99.978% availability and no scheduled downtime.

In order to help answer some of the many questions we receive, we have created this FAQ and a corresponding Google Apps security site. We hope this helps to answer some of your questions about Google's position on these important issues! Be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

How reliable are Google Apps and Google Cloud Platform?

Google Apps offers a 99.9% service level agreement (SLA) for covered services, and in recent years we've exceeded this promise. In 2013, Gmail achieved 99.978% availability. Furthermore, Google Apps has no scheduled downtime or maintenance windows. Unlike most providers, we do not plan for our applications to be unavailable, even when we're upgrading our services or maintaining our systems. Google Cloud Platform has a 99.95% SLA, Google BigQuery Service, and the standard storage class of Google Cloud Storage have a 99.9% SLA except for the Durable Reduced Availability Storage class of Google Cloud Storage which has a 99% SLA.

To minimize service interruption due to hardware failures, natural disasters or other incidents, Google has built a highly redundant infrastructure of data centers. Google Apps has an RPO (Recovery Point Objective) target of zero, and our RTO (Recovery Time Objective) target is instant failover (or zero).

Will my data always be available? What happens in case of downtime?

Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine—or even an entire data center—fails, your data will still be accessible. Google owns and operates data centers around the world to keep the services you use running 24 hours a day, 7 days a week.

How can Google be so reliable?

The application and network architecture run by Google is designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and it uses robust software fail-over to withstand disruption. All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of a machine failure, data will still be accessible through another system. We also replicate data to secondary data centers to ensure protection from data center failures.

What does Google do to plan to plan for disasters or the departure of key staff?

Google has a business continuity plan for its data centers and production operations. This plan accounts for major disasters such as earthquakes and public health crises, and it assumes people and services may be unavailable for up to 30 days . This plan is designed to enable continued delivery of our services to our customers.

How does Google support peaks in demand for Google Apps or Cloud Platform?

Google's services are designed for millions of users. We run multiple different performance tests, including load testing our applications under high load over a long period, to observe effects on factors such as memory use and response time. Google also performs stress testing to examine system performance in unusual situations, including system functional testing while under unusually heavy loads, heavy repetition of certain actions or inputs, input of large numerical values and large, complex queries to a database system.

How will Google guarantee that my data is not accidentally deleted?

Once a client administrator or end-user has deleted data in Google Apps, our Google systems will delete it according to our Privacy Policy or your Google Apps agreement (including the Data Processing Amendment for customers who execute it). The pointer's to a user's data is deleted immediately once a client's administrator deletes a user account. See the Help Center for best practices for deleting users. If you need to recover email messages or data stored in Google Drive, Google offers specific archiving products that complement Google Apps for Work, Government and Education. For other data recovery solutions, be sure to consult the Google Apps Marketplace, where one of our partners may have a solution that meets your needs.

What if I want to leave Google and take my data or application?

We provide tools to make it easy tools to make it easy for you to take your data with you if you choose to stop using our services altogether, without penalty or additional cost imposed by Google. 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 from Google Apps. Google Cloud Platform customers can extract their data using industry standard tools, for which there may be charges.

Compliance

We are proud to comply with regulations across the world and across various sensitive sectors of activity such as healthcare and education. You can use our services with confidence that Google provides the tools and protections you need to meet your compliance requirements

In order to help answer some of the many questions we receive, we have created this FAQ and a corresponding Google Apps security site. We hope this helps to answer some of your questions about Google's position on these important issues! Be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

How can I verify Google Apps' and Google Cloud Platform's security?

Our customers and regulators expect independent verification of security, privacy and compliance controls. Google undergoes several independent third party audits on a regular basis to provide this assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations. Google solutions have regular audits for the following standard:

- (SOC1) (SSAE-16/ISAE-3402): Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- (SOC2): Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- (SOC3): Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- ISO27001: Google Apps , Google Compute Engine, Google Cloud Storage, Google Application Engine, Google DataStore, Google Big Query, Google Cloud SQL
- HIPAA: Google Apps , Google Compute Engine, Google Cloud Storage, Google Big Query, Google Cloud SQL
- FISMA: Google App Engine, Google Apps for Government

Can I obtain a copy of these certificates and audit reports? Where can I download the SOC3 audit report? Where can I see Google's ISO27001 certificate?

The SOC3 Seal of Assurance is published on a certified site and symbolizes that our controls have been examined by an independent accountant. It represents the practitioner's report on management's assertion(s) that the entity's business being relied upon is in conformity with the applicable Trust Services Principle(s) and Criteria. The full SOC3 audit report is also available for download on this certified site. The extensive SOC2 report can be obtained under NDA. The ISO27001 certificate proves 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.

What about the U.S. government? Won't storing data outside of the U.S. mean it won't be subject to U.S. government requests for data?

Storing your data in a particular country does not necessarily protect the data from access by foreign governments. Location of data in one jurisdiction doesn't necessarily mean that another can't compel its disclosure. Moreover, there are reports of government attempts to directly tap cable lines between data centers in multiple locations around the world. That's why we are advocating for surveillance reform. We refuse to provide governments with access to our systems or to install equipment that gives them access to user data. For more information, please visit Google's Transparency Report.

Where does Google store my data?

Your data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers. Google's computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks.

Can I store healthcare data in Google systems?

Google Apps supports our customers' compliance with the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Customers who are subject to HIPAA and wish to use Google Apps with Protected Health Information (PHI) must sign a Business Associate Agreement (BAA) with Google. Administrators for Google Apps for Business, Education and Government domains can request a BAA before using Google services with PHI. Google offers a BAA covering Gmail, Google Calendar, Google Drive and Google Apps Vault. Google Cloud Platform customers can get a BAA for Compute Engine, Cloud Storage, Cloud SQL, and BigQuery.

Do Google products meet privacy requirements for use by students and children?

More than 30 million students rely on Google Apps for Education. Google Apps for Education complies with the U.S. Family Educational Rights and Privacy Act (FERPA), and our commitment to do so is included in our agreements. We contractually require Google Apps for Education schools to obtain parental consent regarding the use of our service in conformity with the U.S. Child Online Privacy Protection Act (COPPA), which facilitates compliance with COPPA requirements.

Can Google be used by U.S. government institutions?

The Federal Information Security Management Act of 2002 (FISMA) is a U.S. federal law pertaining to the information security of federal agencies' information systems. Google Apps and Google App Engine have received an authorization to operate at the FISMA-Moderate level—the standard level for federal email systems—from the U.S. federal government. Hundreds of U.S. federal, state and local government agencies, are using Google Apps for Government, including the U.S. General Services Administration (GSA), which has migrated over 17,000 employees and contractors to Google Apps for Government.

My organization utilizes PCI/DSS data. What tools are available to help me remain compliant?

Payment Card Industry Data Security Standard (PCI DSS) compliance is a set of policies and technical requirements defined for systems that contain or process credit card information.

Google Apps is not meant to process or store credit card transactions. Therefore, customers may configure controls to prevent emails with credit card information from being sent from Google Apps. This helps our customers maintain PCI DSS compliance. For Google Drive, Vault can be configured to run audits and make sure no credit card information is stored.

What eDiscovery tools are available for my organization to support legal & compliance requests?

Google Vault is an add-on for Google Apps that lets you retain, archive, search, and export your organization's email for your eDiscovery and compliance needs. Vault is entirely web-based, so there's no need to install or maintain any software. With Google Apps Vault, you can:

- Search your domain's email data
- Place user accounts (and related data) on litigation hold to preserve email data
- Manage related searches and litigation holds under a single container, called a matter
- Share matters among authorized users
- Export search results in standard file formats
- Save your search queries
- Set email retention policies for your domain

Can I use Google services with data controlled under the International Traffic in Arms Regulations (ITAR)?

ITAR is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Google does not support use of our services with ITAR-controlled data.

Transparency

Whether it's real-time dashboards to verify systems performance, auditing of data handling processes or information about our datacenters, we're committed to leading the industry in transparency. It's your data, and we want you to know what happens with it so that you always remain in control of it.

In order to help answer some of the many questions we receive, we have created this FAQ and a corresponding Google Apps security site. We hope this helps to answer some of your questions about Google's position on these important issues! Be sure to check Google's Privacy and Terms page for more consumer tools and information relating to consumer privacy.

What do you use my data for?

Google processes your data to fulfill our contractual obligation to deliver our services. Google's customers own their data, not Google. The data that companies, schools and students put into our systems is theirs. Google does not sell your data to third parties. Google offers our customers a detailed Data Processing Amendment that describes our commitment to protecting your data.

How do I know if there was an issue with my data?

For security events that may affect the confidentiality, integrity or availability of systems or data,

Google has an incident management process in place. This process specifies courses of action and procedures for notification, escalation, mitigation and documentation. To help ensure the swift resolution of security incidents, the Google information security team is available 24/7 to all Google employees. Google Support, Security or Product Management will notify the affected customers of incidents that affect the confidentiality, integrity or availability of their data. Once an initial notification is made, follow-up notifications and calls are possible as needed for the affected parties to understand the incident.

Who at Google can look at my data?

Access rights are based on a Google employee's job function and role—using the concepts of least-privilege and need-to-know—commensurate with the employee's defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources. Google requires the use of a unique user ID for each employee. This account is used to identify each person's activity on Google's network, including any access to employee or customer data.

Where is my data stored?

Your data will be stored in Google's network geographically distributed data centers. Google maintains a number of geographically distributed data centers. Google's computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks. Storing your data in a particular country does not necessarily protect the data from access by foreign governments. Location of data in one jurisdiction doesn't necessarily mean that another can't compel its disclosure. Moreover, there are reports of government attempts to directly tap cable lines between data centers in multiple locations around the world. That's why we are advocating for surveillance reform. We refuse to provide governments with access to our systems or to install equipment that gives them access to user data. For more information, please visit Google's Transparency Report. Google Cloud Platform allows customers to choose to store their data in Europe, North America, or Asia. This location must be specified by the customer when they configure their application. If a data location is not specified the GCP services will default to North America.

How do I know how much data Google shares with the government?

We regularly publish Transparency Report detailing how governments and other parties affect your security and privacy online. This is because we think you deserve to know. We have a track record of telling you what's going on and standing up for your rights. We were the first to publish a Transparency Report in 2010, and we now publish information about all types of legal process we receive, including processes issued under national security authorities. We still need more transparency from governments and a better balance between civil liberties and national security.

Can I see if Google services are blocked by any countries or governments?

Google's Transparency Report shows disruptions to Google products and services at any point in more than 30 countries. Causes for these disruptions vary, and include network outages and government-mandated blocks.