Google Workspace for Education data protection implementation guide
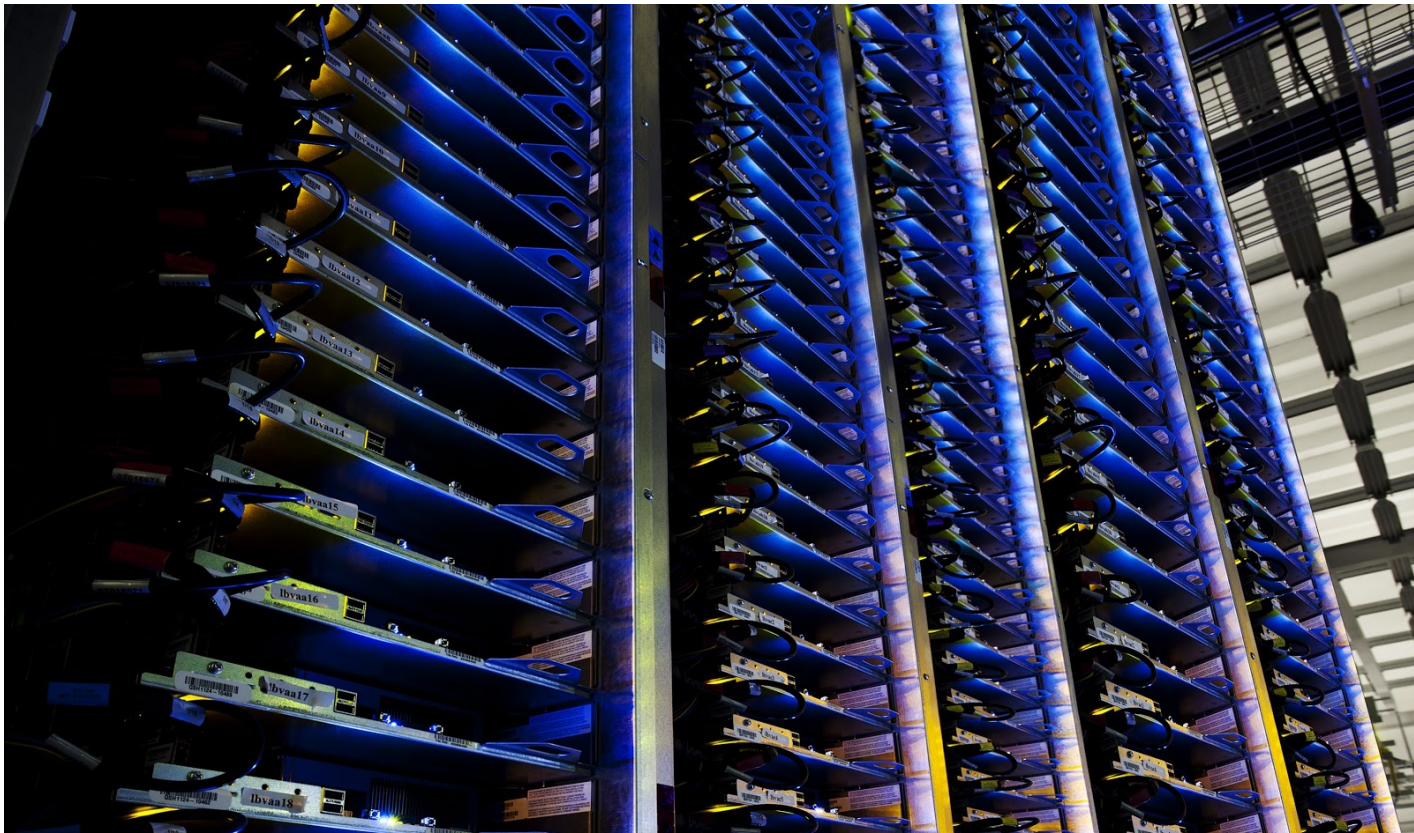
Google Cloud

Google Cloud

Table of contents

Disclaimer

This guide is intended for Google Workspace for Education administrators to help them better understand how to use and customize Google Workspace for Education services and settings to meet data protection compliance needs. We recommend that you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

The content in this guide is correct as of March 2021 and represents the status quo at the time it was written. Google's policies and systems may change going forward, as we continually improve protection for our customers.

Processing Customer Personal Data within our services

Understand your data protection requirements

Google is committed to helping our customers meet their data protection obligations globally—including the requirements set forth by the General Data Protection Regulation (GDPR)—by offering helpful products and tools, by building robust privacy and security protections into our services and contracts, and by providing certifications and audit reports.

Under the Google Workspace for Education [Data Processing Amendment](#) (DPA), Google acts as a processor of the Customer Personal Data that is submitted, stored, sent, or received by your organization via Google Workspace for Education services, and we process such data on your behalf and under your instructions. As a customer, you act as the controller of such Customer Personal Data[1], which means that you determine the purposes and means of processing.

We recommend that you conduct an assessment of your [Google Workspace for Education Agreement](#), the Google Workspace for Education DPA, the [Google Workspace for Education Privacy Notice](#), as well as the terms applicable to any other Google services that you choose to make available for your end users while signed in to their organization managed accounts (for example, the additional services you turned on for your domain).

---

[1] Customer Personal Data means the personal data contained within the Customer Data.

Our Privacy Commitments

Google makes these Cloud [Enterprise Privacy Commitments](#) for Google Workspace for Education products to describe our overarching responsibility to protect your business when you use our enterprise solutions. These commitments are backed by the strong [contractual commitments](#) we make available to you.

- **You control your data.** Customer Data[2] is your data, not Google's. We only process your data according to your agreement(s).

- **We never use your data for ads targeting.** We do not process your customer data or service data to create ads profiles or improve Google Ads products.

- **We are transparent about data collection and use.** We're committed to transparency, compliance with regulations like the GDPR, and privacy best practices.

- **We never sell customer data or service data.** We never sell customer data or service data[3] to third parties.

- **Security and privacy are primary design criteria for all of our products.** Prioritizing the privacy of our customers means protecting the data you trust us with. We build the strongest security technologies into our products.

Google designed Google Workspace for Education to meet stringent privacy and security standards based on industry best practices.[4] In addition to strong contractual commitments regarding data ownership, data use, security, transparency, and accountability, we give you the tools you need to help meet your compliance and reporting requirements (see more information in Appendix 1). Additionally, our [Privacy Commitments](#) provide clarity about our privacy commitments and what you can expect when it comes to protecting and managing your data in the cloud.

Transparency is part of Google's DNA. At Google Cloud, we believe that trust is created through [transparency](#), and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud. At Google Cloud, we strive to create a trusted ecosystem by focusing on three key areas: ensuring the privacy and security of our customers' data, the dependability of our services, and setting—as well as meeting—the highest industry standards around transparency and security.

---

[2] Customer data is the data you, including your organization and your users, provide to Google when you access Google Workspace for Education and the data you create using those services.
[3] Service data is the personal information Google collects or generates during the provision and administration of the Cloud Services, excluding any Customer Data and Partner Data. Service Data is subject to [Google Cloud Privacy Notice](#).
[4] Please see our ISO/IEC certifications (ISO/IEC [27001](#), [27017](#), [27701](#), [27018](#)) as well our [SOC 3](#) Audit Report, available [here](#). For our existing customers who want to learn more about Google's Security, we will be happy to facilitate a detailed [SOC 2 report](#) via the [Compliance Reports Manager](#). You can see the full listing of all of our compliance offerings in our [Compliance resource center](#).

Additionally, we also secure any service data. Service data is the information Google collects or generates while providing and administering Google Workspace for Education and is critical to help ensure the security and availability of our services. Service data does not include Customer Data. Service data includes information about security settings, operational details, and billing information. We process service data for various purposes that are detailed in our newly launched [Google Cloud Privacy Notice](#), such as making recommendations to optimize your use of Google Workspace for Education, and improving performance and functionality.
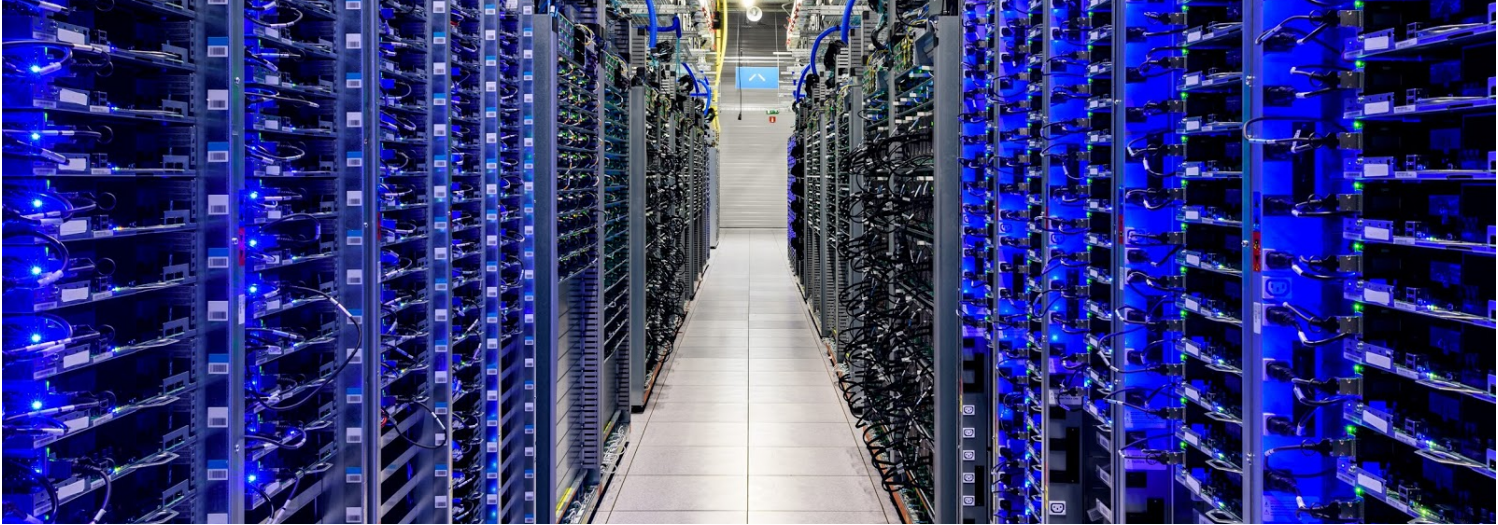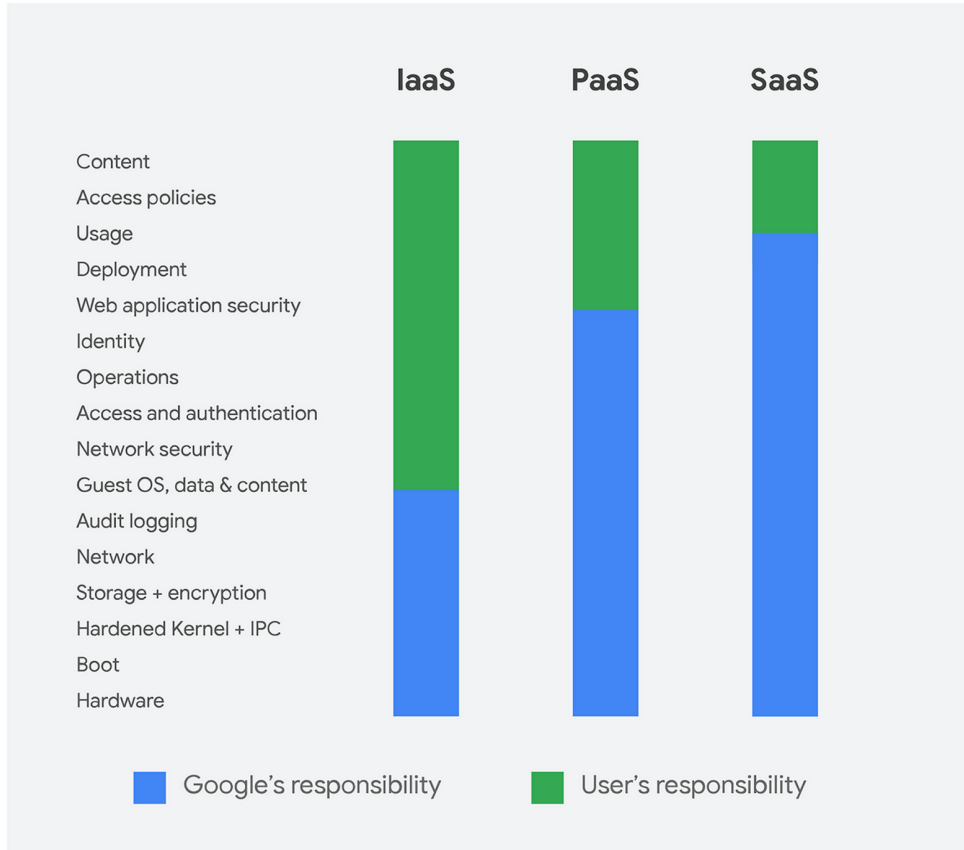

Google Shared Responsibility Model

Data protection is not only the responsibility of the business using Google Workspace for Education services; nor is it only that of Google in providing those services. Data protection in the cloud is instead a shared responsibility; a collaboration between the customer and the Cloud service provider (CSP).

The Google Shared Responsibility Model visually describes the various security responsibilities that our customer and Google are together responsible for Google Workspace for Education is software as a service (SaaS) where almost everything except the content and its access policy is the responsibility of the CSPs. In the SaaS model, CSPs manage all of the physical and virtual infrastructure and the platform layer while delivering cloud-based applications and services for customers to consume. Internet applications that run directly from a web browser or mobile applications are SaaS applications. With this model, customers don't have to worry about installing, updating, or supporting applications—they simply manage system and data access policies.

Important: As a Google Workspace for Education customer, you are responsible for the security of components that you provide or control, such as the content you put in Google Workspace for Education services, and establishing access control for your users.

Google Workspace *for Education (SaaS) responsibility diagram vs. other IaaS and PaaS services*

You can refer to the Shared Responsibility Model as a guide to secure your Customer Data on Google Workspace for Education. Under various data protection regulations, you are responsible for security controls protecting the Customer Personal Data in your possession, monitoring the processing of the Customer Personal Data, monitoring the access to the data, ensuring the accuracy of the data, and managing the lifecycle of the data.

Google protects the infrastructure underlying Google Workspace for Education throughout the information processing lifecycle. Security is provided at each layer through the hardware layer, inter-service communication, inter-service access management, data storage, Internet communication, and operational security. For more information on the topic, please read the Google Infrastructure Security Design Overview whitepaper.

Google services

In this section, we will provide you an overview of various services Google provided to you, including Google Workspace for Education Core Services, embedded features, Additional Services, organization managed Google Account, and technical support services.

- Google Workspace for Education **Core Services**: services listed and described in the services summary
- Google Workspace for Education **Core Services Embedded Features**: embedded in Google Workspace for Education Core Services and are available for all Google Workspace for Education users
- **Feedback**: suggested spelling & grammar corrections feedback and in-product feedback are subject to Google Privacy Policy
- **Additional Services**: not part of the Google Workspace for Education offering, and may be any Google service that can be used with an organization managed Google Account. A non-exhaustive list of Additional Google services is provided here
- **Organization managed Google Account**: an organization managed Google Account is needed for your use of Google Workspace for Education (separate from personal Google Account) and is managed by an administrator
- **Technical Support Services**: Google Workspace for Education admins can contact Google to get technical support services via phone, email, or chat

Google Workspace for Education Core Services

Google Workspace for Education Core Services are the services listed and described in the services summary of the Google Workspace for Education Terms of Service (for example, Classroom, Gmail, Docs, Sheets, and Slides). These are the services provided to Google Workspace for Education customers under your Google Workspace for Education agreement. Learn more about the Google Workspace for Education Core Services here.

The Google Workspace for Education Data Processing Amendment (DPA), as applicable[5], governs how Google processes Customer Data from the Core Services. Customer Data is the data that organizations and their users provide to Google for processing in Google Workspace for Education Core Services, including Customer Personal Data (as defined in the Data Processing Amendment). Customers can opt-in to the DPA in the Google Admin console if you are located outside of Europe and believe it meets your compliance needs.

---

[5] If the GDPR applies to Google's processing of your data—for example, if you are established in the European Union, or established outside the European Union but offer goods/services to data subjects who are in the European Union—it requires your contract with Google to contain certain data processing terms.
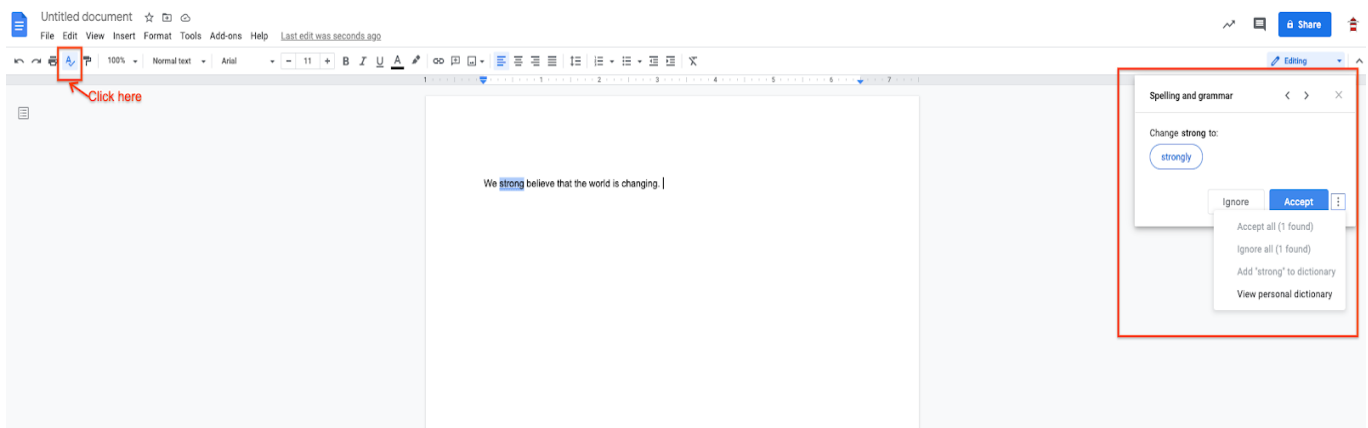
Google Workspace for Education Core Service Embedded Features

The Core Services include a number of features such as spelling & grammar, Explore, Calendar geo-location integration and Translate. These features are embedded in Google Workspace for Education Core Services and are available for all Google Workspace for Education users. Google is a **data processor** of Customer Personal Data processed through the embedded features in Google Workspace for Education Core Services. Features are governed by the Google Workspace for Education DPA when used in conjunction with the Google Workspace for Education Core Services.

Users can choose to turn off some embedded features (for example, turn off autocorrect and suggestions in spelling & grammar in Google Docs and Gmail) or elect not to use the embedded features (for example, "Translate document" and Explore). Please note that if you use Explore to navigate to a third party site, use of the third party site is **not** subject to the protections of the Google Workspace for Education DPA.

Spelling & Grammar

Spelling & grammar is an embedded feature in Google Docs and Gmail. It is important to highlight that your Customer Data is not used to improve spelling & grammar services for other customers' accounts. As highlighted above, Google is a **data processor** in relation to Spelling & grammar where the user accepts or rejects suggested changes. However, if the user takes proactive steps to provide feedback to the suggested spelling and grammar, Google is the **controller** of that feedback data. See below "Feedback" section for more information.

Please note that in addition to the spelling & grammar embedded feature, there are also spell checkers available in Chrome (which is **not** a Google Workspace Core Service). For further information on the basic spell check in Chrome and the enhanced spell check in Chrome, please see "enhanced spell check" section for more information.

Feedback

Please note that any feedback voluntarily provided through our feedback tools will be processed according to the Google Privacy Policy, and we provide users with notice of these terms at all feedback ingress points. Google acts as **controller** for the feedback we collected through feedback. Please remove any personal information and sensitive information before providing feedback to Google.

Users can provide feedback for suggested spelling & grammar corrections (see example below).

Additional info

customer-type
    dasher
customer-id
    ▮▮▮▮▮▮▮
customer-name
    Google.com
storageProvider
    DRIVE
isOwner
    true
editable
    true
commentable
    true
isAnonymousUser
    false
offlineOptedIn
    true
serviceWorkerControlled
    false
devicePixelRatio
    1
zoomFactor
    1
wasZoomed
    false
docLocale
    en
locale
    en
docsErrorFatal
    false
isIntegrated
    false
isPaginatedLayout
    true
isCanvasRendered
    false

We also provide users with an option to provide in-product feedback (for example, in Google Doc). Users may choose to provide screenshots of an issue that they are encountering, and we provide a tool to hide sensitive information.
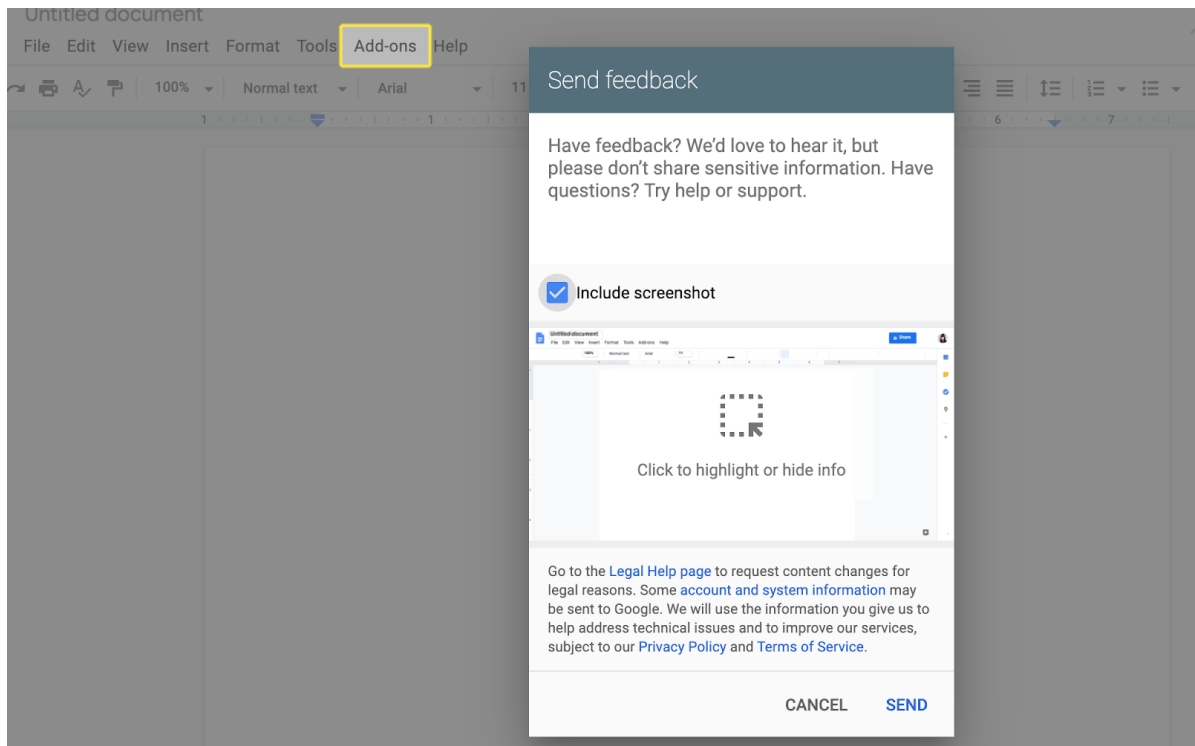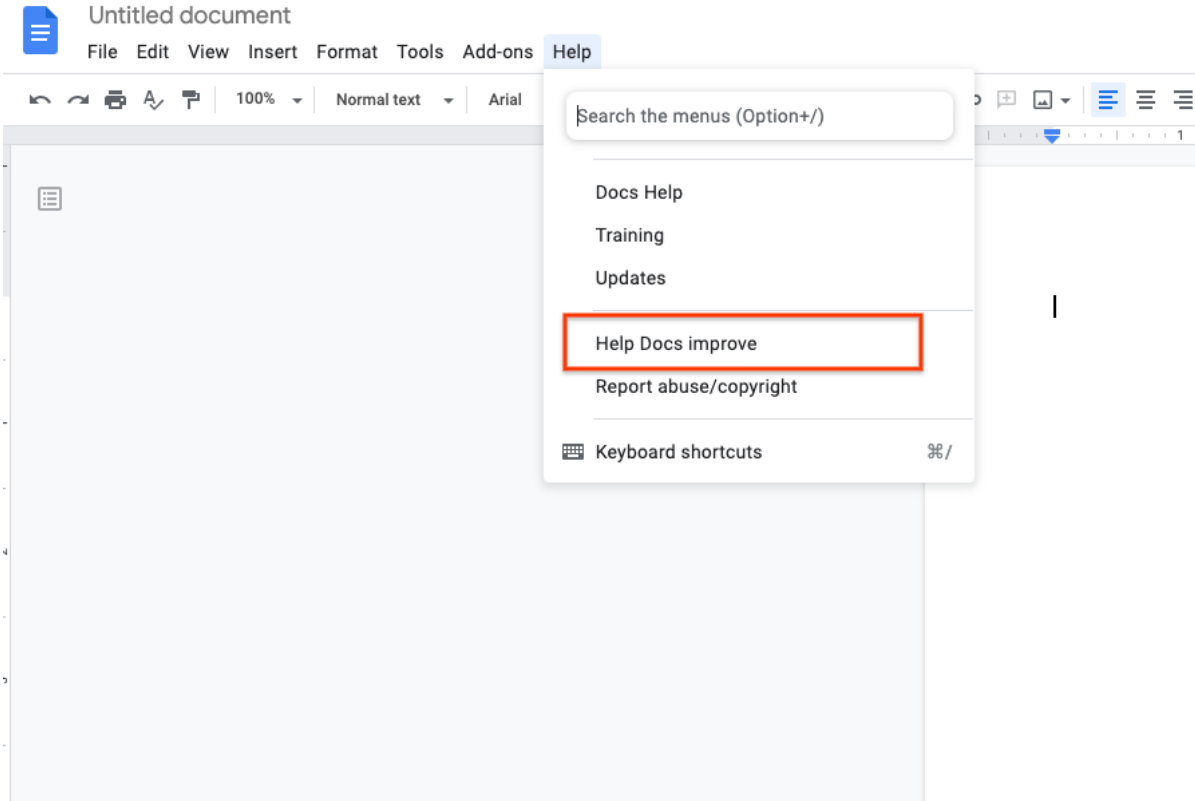
Additional Services

Additional Services are not automatically provisioned as part of the Google Workspace for Education offering, and may be any Google service that can be used with an organization managed Google Account. A non-exhaustive list of Additional Google services is provided here. **Because these services and products are not part of the Google Workspace for Education offering, they are not governed by the Google Workspace for Education DPA and Google Workspace for Education Agreement**.

To offer a smooth experience to Google Workspace for Education customers, Google Additional Services are accessible to users via their organization managed Google Accounts. As detailed on the Additional Services page, most Additional Services are governed by the Google Terms of Service and Privacy Policy, and some Additional Services also have service-specific terms. To review these terms, see Additional Google services and go to the section titled, *Services with an individual On or Off control*. To learn more about Additional Services as it relates to Google Workspace for Education, see here.

> **Important:** Google Workspace for Education administrators might need to turn Additional Services off for users while signed in to their organization managed Google Account for compliance reasons.

Administrators (also called *admins*) can turn each Additional Service *on* or *off* for users in the Google Admin console. These settings can be configured before the admin provisions any user accounts. For instructions, see Additional Google services and go to the section titled, *Turn services on or off for users*. In addition to Google Workspace for Education and other Google services that admins can manage individually with an *on* or *off* control in the Admin console, the admins can manage access to unlisted Google services that don't have an individual control (such as Chromecast, and Google Surveys). For details on how to turn these services On or Off, see manage services that aren't controlled individually.

> **Note:** Even if a Google Workspace for Education admin has turned an Additional Service "Off", users may still access and use some Additional Services in an unauthenticated state or retain some limited functionality, for example, for purposes of accessing purchased content. For example, if the admin has disabled YouTube in the Admin console for the organization, a user can still visit YouTube and use the service in a logged out state, but login using their organization managed Google Account will fail. In this case, Google will not process data that can be linked to the user's organization managed Google Account.

We recommend that your organization's Legal Counsel, Data Protection Officer (DPO), or equivalent, when applicable, should conduct an impact assessment of the processing of Customer Personal Data with these products to determine whether, and how, your organization can fulfill its obligations as a data controller or a data processor, as applicable, for each of these products.

Organization managed Google Account

For users in your organization to use your Google Workspace for Education services, you must give each user an account. An organization managed Google Account gives each user a name and password for signing in to Google services and a profile. Users can provide information directly, when providing a name and profile picture, or indirectly, when Google collects information about when and for what purposes and in what context (app/web, platform and device) a user signs in. When a user signs in to their new organization managed Google Account you created, they receive a notice explaining how their data is collected and accessed by their admin, and how their use of Google Workspace for Education Core Services is governed by your organization's Google Workspace for Education terms. The notice also explains that use of Additional Services when used with the organization managed Google Account are governed by Google Privacy Policy and Google Terms of Service, and applicable service-specific terms. For more information about organization managed Google Account creation, see Options for adding users.

For help setting up your account, creating users, and enabling services, see the Google Workspace for Education Quickstart IT Setup Guide.

Technical Support Services

Online, phone, and chat support is available to Google Workspace for Education admins. Data collected and processed as part of providing technical support services for your use of Google Workspace for Education Core Services are governed by the Google Workspace Technical Support Services Guidelines (TSSG) and Google Cloud Privacy Notice. Google collects and processes data for the purpose of providing the support services described in the TSSG and maintaining those Services. Google has no obligation under the Google Workspace for Education Agreement (or the TSSG) to provide support for any of the Additional Services.

Privacy best practices

In this section, we provide some best practices you can apply for customizing Google Workspace for Education services to meet your organization's data protection compliance needs. Please note this is not a comprehensive and exhaustive list of all potential practices and that tools referenced within this Guide may vary by edition. We recommend that you consult with a legal expert or your organization's data protection officer to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Account setup and settings

Upon account creation, Customers are contractually required to obtain all required consents from end users and, where applicable, parents or guardians, to allow Google's provision of services. For more information about communicating with parents or guardians, see here.

For Google Workspace for Education primary and secondary education (K-12) accounts in particular, the following are recommended account settings:
- Control which third-party & internal apps access Google Workspace data and restrict access to Google Workspace services.
- In Drive, under "Sharing options," turn off external file sharing for students (or restrict external sharing to allow listed domains only) and set "Access checker" to "Recipients only"
- Turn off chat in Docs editors
- In Google Meet, only allow faculty and staff to create meetings. Users who can't create meetings can still join Meet video meetings created by others.
- For all K-12 and higher education accounts, it is recommended to avoid using students' names for email addresses and usernames.

Additional recommendations can be found in the following documents:

- Quickstart IT Setup Guide
- Domain Best Practices
- Deployment Guide

Choose which Additional Services to enable for your users

Additional Services are not part of the Google Workspace for Education offering and are not covered by the Google Workspace for Education DPA and Google Workspace for Education Agreement. Customers are contractually required to obtain all required consents from end users and, where applicable, parents or guardians, to allow Google's provision of Additional Services.

As an admin, we recommend that you carefully choose which Additional Services (for example, YouTube, Maps, and Blogger) to turn on/off for your users, especially for customers with age restrictions or who handle highly regulated or sensitive data (for example, financial data, health data, and government data). Please check the Additional Services section within this Guide for more information.

Admins can also limit access to additional services without an individual on/off control within the Admin Console. By clicking on Additional Google services from the home dashboard, admins can toggle whether access is turned on or off for a certain organizational unit on the left column or leave it at the top level OU which will cover the entire organization.

> ⓘ Access to additional services without individual control for all organizational units is turned Off   **CHANGE**

Clicking the **OFF** toggle will restrict services for that organizational unit. Clicking the **ON** toggle will not restrict services.

Service status   ⌃

Service status   ⦿ OFF for everyone
                          If this setting is Off, users can't access many Google services.
                          Learn more

                        ◯ ON for everyone

                        ⓘ Changes may take up to 24 hours to propagate to all users.

                                                              CANCEL   SAVE

Help your users with their privacy activity controls

Advise your users to opt in to the appropriate activity controls that comply with your school's privacy policies and that meet your users' personal needs. If your users don't wish Google to store their activity history and provide a personalized user experience for their organization managed Google Account, instruct them to turn off certain settings from the Activity controls page. For more details, see the instructions and guidelines below.

- **Location History**—Consider whether you should turn on/off Location History for your users' organization managed Google Accounts. By default, Location History is turned **off** for your users. Location History can only be turned on if you have enabled it in the Google Admin console (after obtaining parental consent where required) **and** if your users have also enabled it. From the Admin console, go to *Apps > Additional Google services > Location History.* Instruct your users to

turn Location History on or off by going to the [Activity controls](#) page for their organization managed Google Account. For user instructions, see [Manage your Location History](#).
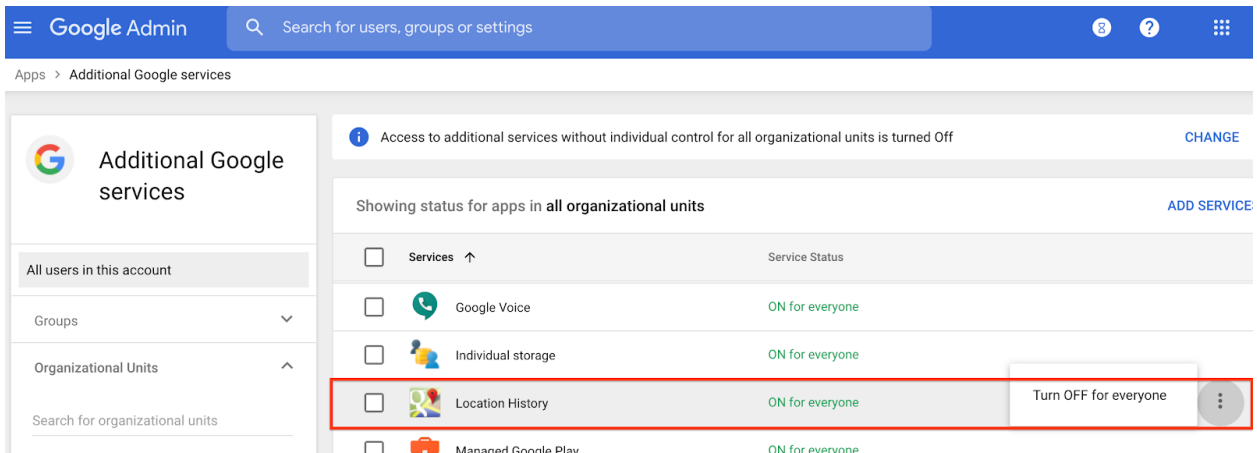
- **YouTube History**—Consider whether you should turn on/off YouTube for your users. For K-12 users, search history is off by default. From the Admin console, go to *Apps > Additional Google services > YouTube*. For Higher Education domains, once you turn on YouTube in the Admin console, your users have options to turn **YouTube History** on or off individually in the [Activity controls](#) page. Any videos they watch while history is off won't show in their history. The history also won't be used to improve their recommendations. For user instructions, see [View, clear, or pause watch history](#).
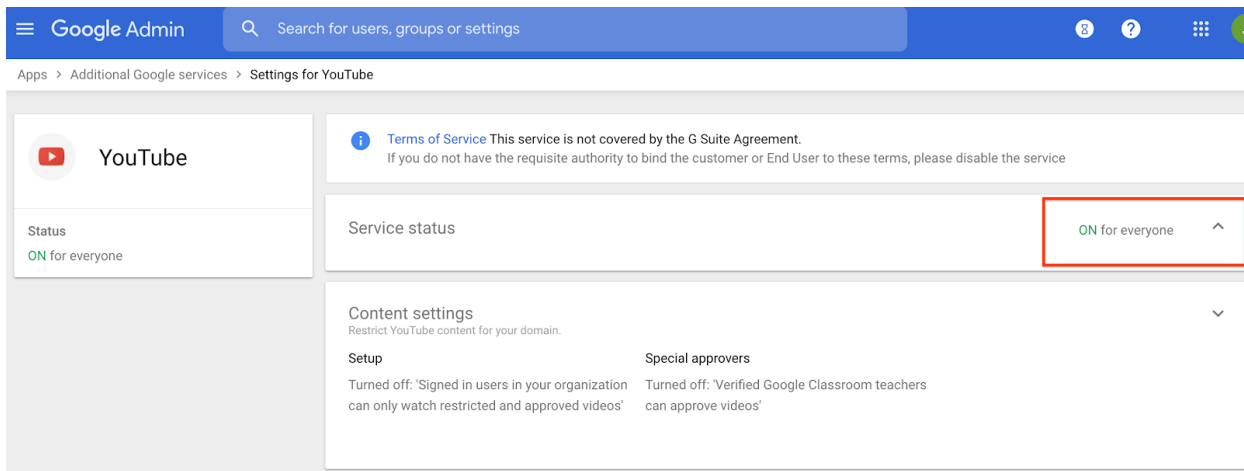
- **Ads -** There are no ads in Google Workspace for Education Core Services and we do not collect or use student data for advertising purposes or create advertising profiles. K-12 Google Workspace for Education users also don't see ads when they use Google Search while signed in to their Google Workspace for Education accounts. Some of Google's additional services such as Blogger and YouTube do show ads to students, however, these ads are not personalized and we give Administrators the ability to [restrict access](#) to these services.

- **Ad personalization**—Ads are based on personal information that a user has added to their organization managed Google Account, data from advertisers that partner with Google, and Google's estimation of a user's interests. For K-12 users, ads personalization is off by default. When Ad personalization is turned on for Higher Education domains, it enables a personalized ad experience for individual users. However, your users have the option to turn on/off this setting from the Activity controls page. When ads personalization is turned off, Google will no longer use their information to personalize their ads. Please consider instructing your users to go to the Activity controls page to turn on/off Ad personalization.

  Note: Google Workspace for Education does not use Customer Data for advertising purposes. Ad personalization is only applicable to Google services offered outside of Google Workspace for Education.
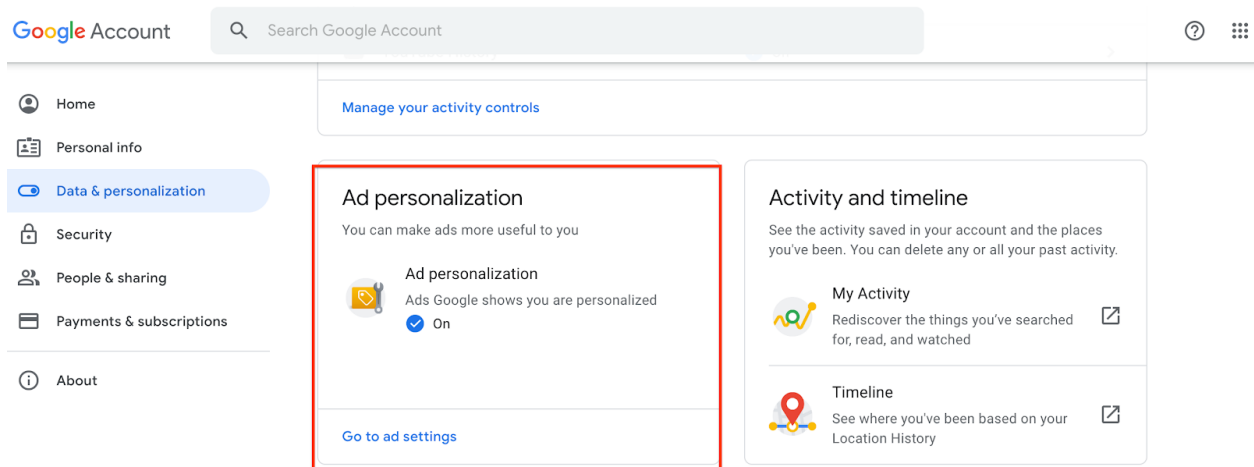
- **Web & App Activity**—Consider whether you should turn on/off Web & App Activity (WAA) for your users. From the Admin console, go to *Apps > Additional Google services > Web and App Activity*. By default, for K-12 accounts, the admin WAA control is off by default and the WAA personalization setting for your end users is turned off. When the WAA service is turned **on** for the organization, the end users have the option to turn it on/off at their preference. If the admin turns the admin WAA control **off** for their organization in the Admin console, end users won't be able to turn it on individually.

  If users choose to turn on the WAA individually, their searches and activity from other Google services are saved in their organization managed Google Accounts, which provides them with a more personalized experience. Users can see and delete their Web & App Activity from the Activity controls page. For user instructions, go to See & control your Web & App Activity.

  Note: As a reminder, there are no ads in Google Workspace for Education core services and we do not use core service student data for advertising purposes or create advertising profiles.
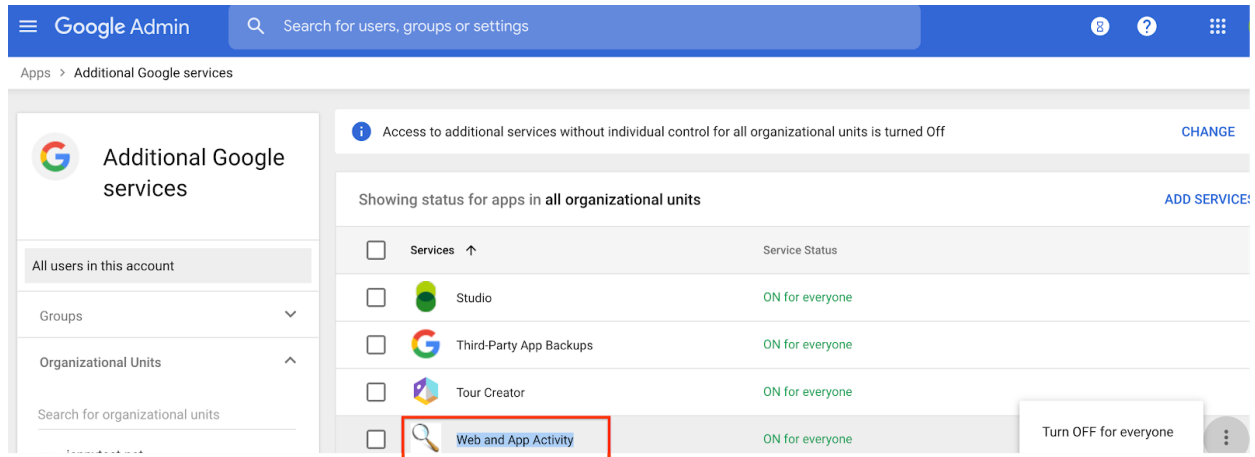
Control which users can use Chrome sync and advice on other Chrome settings

Chrome sync saves your users' bookmarks, history, passwords, and other settings securely to their organization managed Google Accounts and enables your users to access these settings from Chrome on any device. For Google Workspace for EDU domains, Chrome sync is a Core Service. As an admin, you can control who uses Chrome sync from their organization managed account by turning it on/off or let users decide if they want to use sync. When Chrome sync is turned on, users can see and update synced info on any device, like bookmarks, history, passwords, and other settings.

Additionally, admins can also set other features in Chrome to on/off, or let users decide:

- **Help improve Chrome's features and performance**—The transmission of crash reports and usage statistics to Google is enabled by default. Administrators can turn this feature on or off for both ChromeOS or Chrome.[6] Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, Chrome usage statistics do not include web page URLs or personal data. However, if the user has turned on *Make searches and browsing better"* in the Chrome settings, then Chrome usage statistics will include information about the web pages visited by a user, and the user's usage of those pages. If Chrome sync is enabled, Chrome may also combine any declared age and gender information from the user's organization managed Google account with our statistics to help us build better products for all demographics. This information does not personally identify the user and is used only in aggregate form. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal data depending on what was happening at the time the crash report was triggered.

---

[6] On desktop Chrome, the administrator can enable, disable this setting, or give users the choice. On Chrome OS, the administrator must make a decision and can't leave it to the user.

- **Enhanced spell check**—The basic spell check uses a local dictionary, while the enhanced spell check is cloud-based and sends the text that your users type to Google. By default, basic spell check is turned on for your users. If your users want to enable enhanced spell check, they can do so from the Chrome menu by clicking *Preferences > Advanced > Languages*. If the enhanced spell check is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Please note the enhanced spell check is not part of the Google Workspace for Education Core Services, and therefore it's not governed by Google Workspace for Education Agreements and DPA. The data sent back to Google by enhanced spell check is processed in accordance with the [Google Privacy Policy](), and [Chrome and Chrome OS Additional Terms of Service]().

If you've opted into "Make Searches and Browsing Better (sends URLs of the pages you visit to Google)", Chrome sends a request to Safe Browsing each time you visit a page that isn't in Chrome's local list of safe sites in order to gather the latest reputation of that website ("real-time checks"). If you sync your browsing history without a sync passphrase, this request also contains a temporary authentication token tied to your Google account to provide better protections to some users whose account may be under attack. If the website is deemed unsafe by Safe Browsing, you may be shown a warning. This mechanism is designed to catch unsafe sites that switch domains very quickly or hide from Google's crawlers.

Finally, when ChromeOS or desktop users grant websites access to their location, that location is also shared with Google Location Services (GLS). Admins can disable this by disabling Geolocation via Devices > Chrome > Settings > User & Browser Settings > Security > Geolocation.

If your organization needs stricter admin control over Chrome settings and needs to control what data is being shared with Google and third parties through Chrome, please consider using our Chrome Education Upgrade offering. Chrome Education Upgrade gives admins options to set various policies for their organization. For example, admins can set up the Metrics Reporting policy to disable crash-related data being sent to Google for all users in their organization and anonymous reporting of usage.

For more information on Chrome privacy settings, see our Google Chrome Privacy Whitepaper.

Separate user access within the domain

As an admin, you can manage user access to different sets of Google Workspace for Education Services and Additional Products by creating organizational units. By doing this, you can separate into different groups the users who manage personal/sensitive data and the users who don't. Once these organizational units are set up, you can turn on or off specific services/products for groups of users.

For example, the Human Resources (HR) department may manage personal/sensitive data, but only a subset of HR users may actually need access to this data. In this case, you can configure an HR organizational unit for users using Google Workspace for Education Core Services with personal/sensitive data, with certain services disabled and settings configured appropriately.

Advise users to keep organization managed Google Accounts and personal accounts separate

We recommend that users keep the access to their organization managed Google Account and personal Google Account separate from each other. As an admin, we recommend that you advise users not to sign in to multiple Google Accounts simultaneously in the same Chrome browser. Users can also sign into their Google Workspace for Education account as a secondary account. This mitigates the risk of human error that leads to the accidental storage of Customer Data in a user's personal account or the application of privacy settings from a personal Google Account to an organization managed Google Account.

If your organization needs stricter control, you can prevent users from signing in to Google services using any accounts other than those you provide them with. For example, you might not want users to use their personal Gmail account or an organization managed Google Account from another domain. For instructions, see Block access to consumer personal accounts.[7]

Additionally, as an admin you can securely manage school apps and data on Android devices and leave personal apps and data under the user's control. A work profile[8] can be set up on an Android device to separate work apps and data from personal apps and data. Learn more about how to set up the work profile and allowlist preferred work apps for Android devices.

Review security health recommendations

To increase the safety and security of your organization's data, consider reviewing the recommendations provided by the security health page in the Admin console. You can also check the security checklist for medium and large businesses in the Admin Help Center.

Admins also have many powerful security tools at their disposal and are empowered to customize their individual security settings to meet their business needs. For example, the Alert Center for Google Workspace for Education provides alerts and actionable security insights about activity in your domain to help protect your organization from the latest security threats, like phishing and suspicious device activity. The security investigation tool allows you to identify, triage, and take action on security and privacy issues in your domain. Admins can also automate actions in the investigation tool by creating activity rules to detect and remediate such issues more quickly and efficiently. In addition, Google Vault allows you to retain, hold, search, and export data in support of your organization's retention and eDiscovery needs. These and many more security tools are available and detailed within the Google Workspace Security page.

---

[7] You need to sign up the Chrome Browser Cloud Management to set group policies for enrolled browsers.
[8] Setting up a work profile requires advanced mobile management. Learn more about how to set up advanced mobile management.
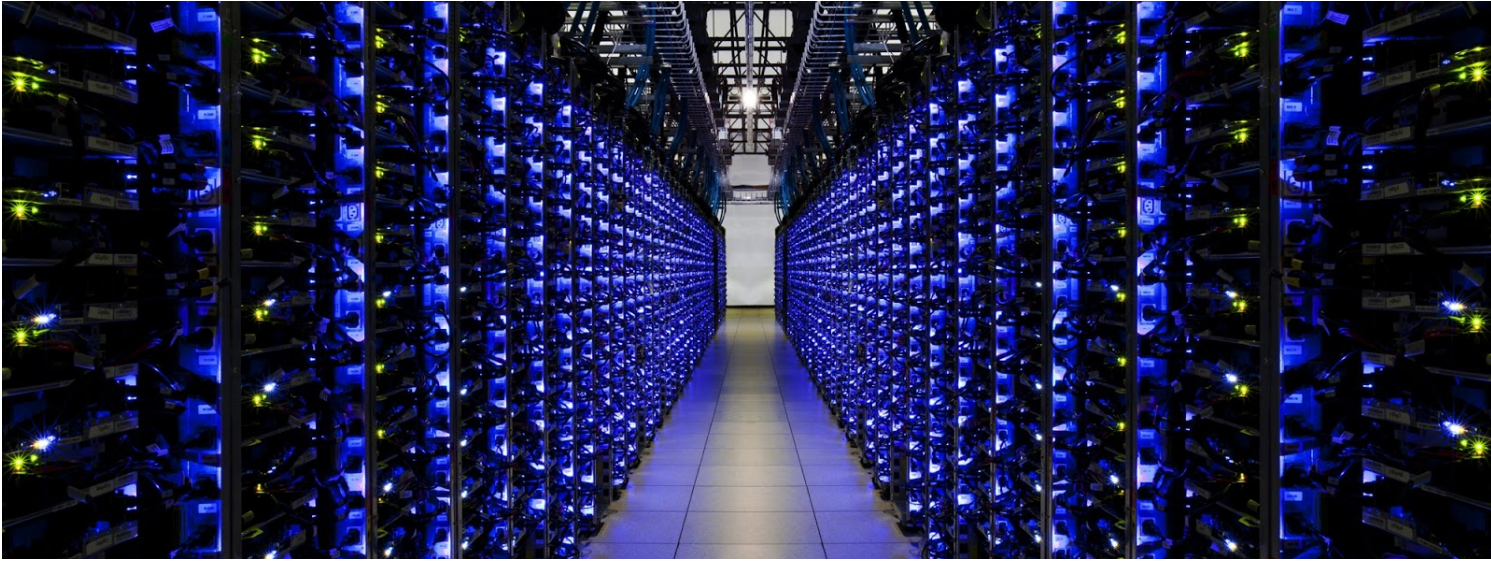
Review your organization's use of third-party applications

Some Google Workspace for Education services may make it possible for a user to share Customer Personal Data with a third party (or a third-party application) based on your settings for the domain. As such, customers are responsible for ensuring that appropriate, compliant measures are in place with any third party (or third-party application) before sharing or transmitting Customer Personal Data. Your organization is responsible for determining whether any other data-protection terms need to be in place before sharing personal/sensitive data with the third party using Google Workspace for Education services, or applications that integrate with them.

As an admin, you have three choices in managing the Google Workspace Marketplace. You can prohibit the installation of all apps, allow only the installation of allowlisted apps, or allow the installation of any app. Admins can also choose to install apps, and grant consent for these apps, on behalf of Google Workspace for Education users. By default, Google Workspace for Education primary/secondary (K-12) users are prevented from installing all apps. We recommend that you review the school policy and allowlist only selective third-party applications that can access API scopes across Google Workspace for Education services.

Using app access control, you can further control which third-party and domain-owned apps can access sensitive Google Workspace for Education data. Use app access control to:

- Restrict access to most Google Workspace for Education services, or leave them unrestricted.
- Trust specific apps so they can access restricted Google Workspace for Education services.
- Trust all domain-owned apps.

We recommend that you review the school's policy and change the setting to restricted or limited access to your Google Workspace for Education Customer Data if needed.

Monitor account activity

Admin console reports and audit logs make it easy to examine potential security risks, measure user collaboration, track who signs in and when, analyze admin activity, and much more. To monitor logs, admins can configure notifications to send them alerts when Google detects certain activities—including suspicious login attempts, users suspended by an admin, new users who are added, suspended users who are made active, users who are deleted, password changes by an admin, users who are granted an admin privilege, and users who have their admin privilege revoked. The admin can also review reports and audit logs on a regular basis to examine potential security risks. In particular, the key trends in the highlights section, overall exposure to data breaches in security, files created in apps usage activity, account activity, and audits provide helpful security risk insights.

While admin audit logs provide information about actions taken by members within your own organization, Access Transparency[9] provides logs of the actions taken by Google personnel. The access transparency logs include information about the accessed resource and action, the time of the action, and the reason for the action (for example, the case number associated with a customer support request).

Establish privacy policies for file names and path names

As an additional security precaution, to restrict sharing of Customer Personal Data, we recommend that you establish policies to prevent users from including sensitive information when naming and organizing files in Google Workspace for Education Core Services (for example, Docs, Sheets, Slides, Forms, Drive, Gmail), or naming the Google Chat room or Meet invite with sensitive personal information. Examples of sensitive Customer Personal Data includes an individual's full name, email address, mailing address, telephone number, or any unique account identifiers (for example, customer ID, project ID, and screen name).

Additionally, you can take advantage of data loss prevention (DLP) capabilities in Google Workspace for Education to inspect, classify, and de-identify sensitive data to help restrict exposure. See Prevent data loss using DLP for Drive and Scan your email traffic using DLP rules. We provide a library of predefined content detectors to make setup easy. Once the DLP policy is in place, for example, Gmail can automatically check all outgoing email for sensitive information and automatically take action to prevent data leakage: either quarantine the email for review, tell users to modify the information, or block the email from being sent and notify the sender. With easy-to-configure rules and optical character recognition (OCR) of content stored in images, DLP for Drive makes it easy for administrators to audit files containing sensitive content and configure rules that warn and prevent users from sharing confidential information externally. Learn more in our DLP whitepaper.

---

[9] This feature is only available with Google Workspace for Education Standard and Plus.

COPPA

The Children's Online Privacy Protection Act of 1998 (COPPA) is a U.S. regulation applicable to the collection of personal information from children under the age of 13. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Google Workspace for Education Core Services can be used in compliance with COPPA. Google contractually requires that schools using Google Workspace for Education and any Additional Services, if applicable, obtain parental consent required under COPPA.

FERPA

Student educational records are protected under FERPA (The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99). This federal law applies to any school with certain programs funded by the U.S. Department of Education.

Google Workspace for Education can be used in compliance with FERPA, our commitment to which is included in our agreements.

Online safety

It's important that children know about online safety and how to safeguard their valuable information, recognise scams and phishing attempts, and keep private information private. Our Be Internet Awesome Family Guide gives families tools and resources to learn about online safety and citizenship at home. Our Digital Wellbeing Family Guide helps you start a conversation about tough tech questions and navigate the digital world as a family. Parents and guardians may also find the Parent and Guardian Security Resource helpful.

Additional resources

To help our customers with compliance and reporting, we share privacy-related instructions and best practices, and provide easy access to documentation. Our products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn your trust. For a list of Google Workspace for Education standards, regulations, and certifications, see our [Compliance resource center](#).

For easy, on-demand access to these critical compliance resources, at no additional cost, see our [Compliance Reports Manager](#). Key resources include our latest ISO/IEC certificates, SOC reports, and self assessments. Select resources may require sign-in with your Google Cloud Platform or Google Workspace for Education account.

For more information on how Google Workspace for Education services are designed with privacy, confidentiality, integrity, and availability of data in mind, see the following:

- **Google Cloud Privacy** - Includes the list of Enterprise Privacy Principles for Google Cloud
- **Google Workspace Security page** - Homepage for Google Cloud security, with links to security white papers and other resources related to privacy, transparency, infrastructure, and security products
- **Google Workspace Admin Help Center** - Homepage that links to instructions and technical documentation for Google Workspace products and security features
- **GDPR Resource Center** - Includes regulatory, compliance, and product information to help you with GDPR compliance
- **Security resource center** - Includes whitepapers, videos, articles, blog posts, and documentation on privacy and security
- **Google for Education Privacy & Security Center** - Resource for Google Workspace for Education customers.
- **Google for Education Guardian's Guides to Google Tools** - Digital resources to help parents support their child's learning from home

Appendix 1: Privacy control mapping

This privacy control mapping provides a convenient way to assess what you need to support requirements from various privacy regulations when using Google Workspace for Education. Please note this is not an exhaustive list of all privacy controls, but is intended as a general high-level mapping. We recommend that you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Data controller considerations

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
Understanding the organization and its context	The organization shall determine its role as a Personally Identifiable Information (PII) controller and/or a PII processor to identify the appropriate requirements (regulatory, etc.) for processing Customer Personal Data.	See the roles and responsibilities when processing Customer Data in section 5 of the Google Workspace for Education Data Processing Amendment.
Determine when consent is to be obtained and record consent	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing Customer Personal Data, and record the consent when needed.	Google does not provide support for gaining and recording user consent for all of your activities. When users sign in to the organization managed Google Account you created, they receive a notice explaining how their data is collected and can be accessed by their admin.
Identify lawful basis and document purpose	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be collected. The customer should document the purpose for which Customer Personal Data is processed.	Google does not provide support for gathering the lawful basis of processing for all of your activities. To learn about the processing activities Google performs for you, and the purposes of that processing, see the Google Workspace for Education Agreement and Data Processing Amendment.
Contracts with PII processors	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to	As your data processor, Google will assist you in ensuring compliance with your obligations (taking into account the nature of the processing of Customer Personal Data and the information available to

	processing and protecting Customer Personal Data.	Google) in accordance with the [Data Processing Amendment](). See Section 7.1.4 (security assistance), 9.2.2 (data subject rights assistance), and 8.1 (DPIA assistance) for more information.
Limit collection and processing	The customer should understand requirements around limits on collection and processing of Customer Personal Data (e.g., that the collection and processing should be limited to what is needed for the specified purpose).	To learn about the processing activities Google performs for you, and the purposes of that processing, see the [Google Workspace for Education Agreement]() and [Data Processing Amendment]().
Records related to processing PII	The customer should maintain all necessary and required records related to processing Customer Personal Data.	Google Workspace for Education provides audit logs to give you visibility on the data access and help you answer such questions as, *Who did what, where did they do it, and when did they do it?* Available audit logs include admin activity logs (admin audit log), security logs (login, SAML, and access transparency), and user services and account logs (email log search and Drive audit log). To learn more about audit logs, see [available audit logs](). The general retention time for audit logs is 6 months (for details, see [Data retention and lag times]()). You can [customize what you review for any audit log]() in your Google Admin console by filtering by user or activity, organization unit, or date. You can also set up alerts for certain activities.

Organizational data protection policy and assessment

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
Independent review of information security	The customer shall apply an information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability. This may include internal or external audits, or other measures for assessing the security of processing. Where the	You are responsible for your use of the services and your storage of any copies of Customer Data outside of Google systems or Google's [subprocessors']() systems. Google undergoes an increasing amount of independent third-party audits on a regular basis. For each one, an

	customer is dependent on another organization or third party for all or part of the processing, they should collect information about such assessments performed by them.	independent auditor examines our data centers, infrastructure, and operations. Regular audits are conducted to certify our compliance with the auditing standards ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, and SOC 2. For a list of compliance certifications, see the Google Cloud Compliance resource center. Based on your contract terms with Google as a Google Workspace for Education customer, Google may allow you—or an independent auditor appointed by you—to conduct audits (including inspections) to verify Google's compliance with its obligations, in accordance with section 7.5 (Reviews and Audits of Compliance) in the Data Processing Amendment.
Data protection impact assessment (DPIA)	The customer should be aware of requirements for completing a data protection impact assessment (when they should be performed, what needs to be included in the assessment, and who should perform the assessment, etc.).	As your data processor, Google will assist you in ensuring compliance with its obligations around data protection impact assessment (taking into account the nature of the processing and the information available to Google) in accordance with section 8 of the Data Processing Amendment.
Determining the scope of the information security management system	As part of any overall security or privacy program that a customer may have, they should include the processing of Customer Personal Data and requirements relating to it. Policies for system development and design should include guidance for the organization's PII processing, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization.	Google does not provide support for its customers' internal process. At least annually, consider creating privacy policies and associated training materials to disseminate to users and privacy groups across your organization. Google offers Professional Services options for educating users on cloud security and privacy, including but not limited to a Google Workspace Security Assessment.
Information security policies	The customer should augment any existing information security	Google does not provide support for its customers' internal process.

	policies to include protection of Customer Personal Data, including policies necessary for compliance with any applicable legislation. The customer should determine and assign responsibility for providing relevant training related to protecting Customer Personal Data.	Consider developing an org-wide security and privacy assessment and authorization policy that defines the procedures and implementation requirements of organization privacy assessments, privacy controls, and authorization controls.
Organization of Information Security Customer consideration	The customer should, within their organization, define responsibilities for security and protection of Customer Personal Data. This may include establishing specific roles to oversee privacy-related matters, including a Data Protection Officer (DPO). Appropriate training and management support should be provided to support these roles.	Google does not provide support for its customer internal process. Consider appointing one or more persons responsible for developing, implementing, maintaining, and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII (Personally Identifiable Information). You can designate your data protection officer and EU representative in the Google Admin console at **Account Settings > Legal and Compliance**. Google has designated a DPO for Google LLC and its subsidiaries, to cover data processing subject to various privacy regulations.
Classification of information	The customer should explicitly consider their use of PII as part of a data classification scheme.	Google does not provide support for its customers' internal process. Your information classification system should explicitly consider your use of PII as part of the scheme that you implement. Considering PII within the overall classification system is integral to understanding what type or special categories of PII that you process, where such PII is stored, and the systems through which it can flow. Your data classification scheme should describe how you classify data, depending on its sensitivity and identifiability. Data owners are

		responsible for determining the appropriate data classification based on who requires access and for what purposes, the potential risks and harm if the data is subject to unauthorized access, as well as the general context of the data.
Management of information security incidents	The customer should have processes for determining when a Customer Personal Data breach has occurred. The customer should understand and document their responsibilities during a data breach or security incident involving Customer Personal Data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	We recommend that you establish an incident response policy for your organization, including procedures to facilitate and implement incident response controls, and that you create security groups for your organization's incident response teams and authorities. We also recommend that you develop an incident response test plan, procedures, checklists, requirements and benchmarks for success. Consider specifying classes of incidents that should be recognized by your organization, and outline the associated actions to take in response to such incidents. Consider also defining the specific actions that should be taken by authorized personnel in the event of an incident, such as steps for managing information spills, cybersecurity vulnerabilities, and attacks. Additionally, take advantage of capabilities in Google Workspace for Education to scan and quarantine email content, block phishing attempts, and set restrictions on attachments. You can also use data loss prevention (DLP) to inspect, classify, and de-identify sensitive data to help restrict exposure. See Prevent data loss using DLP for Drive, Scan your email traffic using DLP rules, and DLP whitepaper. As a Google customer, Google will notify you promptly after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data. See our commitment in section 7.2 (Data

		Incident) of the Data Processing Amendment. See also our data incident response process.
Information backup	The customer should have a policy that addresses the requirements for backup, recovery, and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g., contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements.	We recommend that you develop a contingency plan for your organization that defines the procedures and implementation requirements for contingency planning controls across your organization. We also recommend that you identify key contingency personnel, roles, and responsibilities across organizational elements. Additionally, highlight the mission-essential and business-essential information system operations within your organization. Outline recovery time objectives (RTO) and recovery point objectives (RPO) for resuming essential operations once the contingency plan has been activated. Document critical information systems and associated software. Identify any additional security-related information, and provide guidance and requirements for storing backup copies of critical system components and data. Google owns and operates data centers all over the world, helping to keep the internet humming 24/7 and providing redundancies and resilience to our customers. You can also deploy additional backup and sync from your local files to Google Drive.

Data protection & security settings

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
User access management (including user access provisioning, and management of	The customer should be aware of which responsibilities they have for access control within the	We recommend that you develop an org-wide access control policy for information system accounts in the

privileged access)	service they are using, and manage those responsibilities appropriately, using the tools available.	cloud. We recommend that you define the parameters and procedures by which your organization will create, enable, modify, disable, and remove information from system accounts. The Google Admin console provides you with centralized administration, which makes setup and management more efficient. You can protect your organization with security analytics and best practice recommendations within the security center. You can use Cloud Identity and Access Management (IAM) to assign roles and permissions to administrative groups, using the methodology of least privilege and separation of duties. Learn how to add Cloud Identity to your Google Workspace Account.
Secure log-on procedures	The customer should provide the capability for secure log-on procedures for any user accounts under its control.	As a Google Workspace for Education customer, you can use integrated Cloud Identity features to manage users and set up security options like 2-step verification and security keys. With 2-step verification, you add an extra layer of security to Google Workspace for Education accounts by requiring users to enter a verification code in addition to their username and password when they sign in. The 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 organization managed Google Account. It sends an encrypted signature rather than a code, and helps ensure that your login cannot be phished. For details, see How to use a security key for 2-Step Verification. For additional user authentication/authorization features,

		see the Google Cloud Security and Compliance Whitepaper.
Event logging and protection	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to Customer Personal Data that they deem necessary. A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts.	Google Workspace for Education provides audit logs to help you answer such questions as, *Who did what, where did they do it, and when did they do it?* Available audit logs include admin activity logs (admin audit log), security logs (login, SAML, and Access Transparency), and user services and account logs (email log search and Drive audit log). To learn more about audit logs, see Available audit logs. The general retention time for audit logs is 6 months (for details, see Data retention and lag times). You can customize what you review for any audit log in your Google Admin console by filtering by user or activity, organizational unit, or date. You can also set up alerts for certain activities.
Encryption	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	Google Workspace for Education Customer Data is encrypted in transit, at rest, and on backup media. Encryption is an important piece of the Google Workspace for Education security strategy, helping to protect your emails, chats, Google Drive files, and other data. Additional details on how data is protected at rest, in transit, and on backup media, and details on encryption key management can be found in our Google Workspace Encryption Whitepaper. As an admin, if your organization needs additional encryption on outgoing email, you can set up rules to require outgoing messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME). This helps to ensure appropriate security, confidentiality, and integrity of Customer Personal Data.

Records of countries and organizations to which PII might be transferred	The customer should understand, and be able to provide to the individual, the countries to which Customer Personal Data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	Google owns and operates data centers around the world to keep its products running 24 hours a day, 7 days a week. For more details, see Discover our data center locations. You can choose to store your data in a specific geographic location (the United States or Europe) by using a data region policy. This service provides fine-grained control of the geographical location for storage of email messages, documents, and other Google Workspace for Education content. Please review our data regions product offering carefully and consult with legal counsel to make your own assessment as to whether it meets your specific compliance or business needs.
Records of PII disclosure to third parties	The customer shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Google and its affiliates use a range of *subprocessors* to assist with the provision of its services. For details, see our disclosure of Google Workspace subprocessors. As an admin, we recommend that you evaluate the use of third-party applications. You have the option to disable users from installing third-party applications, such as Google Drive apps and Google Docs add-ons. We recommend that you review the security documentation provided by third-party developers, as well as the applicable data processing terms, before using any such third-party applications with Google Drive and Google Docs. If Google receives a government data request for Cloud Customer Data, it is Google's policy to direct the government to request such data directly from the Cloud customer. We have a team that reviews and evaluates each request we receive to make sure it satisfies legal requirements. When compelled to produce data, Google promptly notifies

		customers before any information is disclosed, unless such notification is prohibited by law or except in emergency situations involving a threat to life. Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request. Detailed information is available in our Transparency Report and Google Cloud Government Requests Whitepaper.
Determining data subjects' rights and enabling exercise (including access, correction, erasure, export)	The customer should understand requirements around the rights of individuals related to the processing of their Customer Personal Data. These rights may include things such as access, correction, erasure, and export. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g., to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	As a Google Workspace for Education Administrator, you can use the Google Admin console to help you fulfill potential obligations related to Data Subject Requests (DSRs). Google Workspace for Education provides functions for both Google Workspace for Education admins and data subjects to access and export customer personal data from Google products directly. Google Workspace for Education admins can use the Data Export tool to export organization level data, and use Google Vault for targeted user-based searches and export. Data subjects (users) can use the Google Takeout interface to directly access and export customer personal data by themselves. For instructions, see the Google Workspace Data Subject Requests Guide.

Retention and deletion	The organization that processes PII should ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period.	As an admin, Google will follow your instructions to delete the relevant Customer Data from Google's systems. Admins can manage user accounts through the Google Admin console, including deleting an account or removing customer personal data from mobile devices and products. If your organization is required to preserve data for a period of time, you can configure Vault to retain it even if users delete messages and files, and then empty their trash. For instructions on deletion settings, see the Google Workspace Data Subject Requests Guide. See our commitment for data deletion in section 6 (Data Deletion) of the Data Processing Amendment. Please check out Google Cloud Privacy Notice for the deletion and retention of service data.
Endpoint management	The customer should ensure that the use of mobile devices does not lead to a compromise of PII.	As an admin using Google endpoint management, you can make your organization's data more secure across your users' mobile devices, desktops, laptops, and other endpoints. With basic management, you can set up basic passcode enforcement, mobile reports, hijacking protection, remote account wipe, and device audits and alerts. With advanced management, you get additional security and privacy features such as strong password enforcement, the blocking of compromised devices, device approval, and more. For more details and to choose the proper device management version, see Compare mobile management features. See also Set up basic mobile device management and Set up advanced mobile management.