Google classroom policy

Google Classroom is a free web service developed by Google and part of the G Suite for Education to help schools streamline the process of sharing files between teachers and students. Students using Google Classroom can view assignments, submit homework, and receive grades from teachers to help them stay on track and organized. The G Suite for Education core services are the heart of Google's educational offering to schools. The core services include Gmail, Calendar, Classroom, Contacts, Drive, Docs, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault. More than 50 million students, teachers and administrators in almost every country in the world rely on G Suite to learn and work together.

Google's terms state they use information to help improve the safety and reliability of the services. G Suite for Education requires users create a Google Account which is created and managed by a school for use by students and educators. Google's terms state they are fully committed to the security and privacy of users' data and protecting users and schools from attempts to compromise it. Lastly, Google's terms state they make contractual commitments in their G Suite for Education agreement and commit to comply with privacy and security standards.

Google Classroom can be accessed through its website, and is available for download at the iOS App Store and the Google Play Store. The Privacy Policy (which takes effect on January 22, 2019) and Terms of Service used for this evaluation can be found on Google Classroom's website, iOS App Store, and the Google Play Store. This evaluation only considers policies that have been made publicly available prior to an individual using the application or service.

This evaluation is intended to provide key information about Google Classroom's collection and use of data for G Suite for Education users. Where there are terms that differ, as with the limitations on advertising in G Suite for Education, the G Suite for Education Agreement takes precedence, followed by the G Suite for Education Privacy Notice, and then the Google Privacy Policy.

Additionally, other relevant policies used for this evaluation include:

- G Suite Service Specific Terms
- G Suite for Education: Privacy and Security
- Google Education Privacy and Security
- Our Privacy and Security Principles
- Data Processing Amendment to G Suite and/or Complementary Product Agreement
- G Suite Service Level Agreement
- G Suite Technical Support Services Guidelines
- G Suite Services Summary
- G Suite for Education Core and Additional services
- Communicating with Parents and Guardians about G Suite for Education
- Notice template for schools when gathering parent or guardian consent
- Legal Frameworks For Data Transfers
- Google's Partners
- Google's subprocessors
- Google Advertising
- Type of cookies used by Google
- Export your organization's data
- Compliance amendments for G Suite and Cloud Identity
- Google Cloud Privacy
- Google Cloud Security

Safety

Google's terms state they use information to help improve the safety and reliability of the services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, its users, or the public. A school may allow students to access Google services such as Google Docs, Sheets, Slides and Sites. These services enable students to collaborate with their peers and teachers in real-time, allowing them to share their work, get feedback, and make edits instantaneously. They can be kept private, shared with others (such as a parent, or the entire class), or even made public. When users share information publicly, it may be indexable by search engines, including Google. The services provide users with various options for sharing and removing content.

Privacy

G Suite for Education requires users create a Google Account which is created and managed by a school for use by students and educators. The terms state when creating this account, the school may provide Google with certain personal information about its students and educators, which includes a user's name, email address, and password in most cases, but could also include secondary email, phone, and address if the school chooses to provide that information. Google may also collect personal information directly from users of G Suite for Education accounts, such as telephone number, profile photo or other information they add to a G Suite for Education account.

The G Suite for Education core services include Gmail, Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts, Vault, and Chrome Sync. These services are provided to a school under its G Suite for Education agreement. Besides the Core Services, G Suite for Education users may have access to other Google services that are generally available for consumers, such as Google Maps, Blogger, and YouTube. The terms call these "additional services" since they are outside of the G Suite for Education core services.

For G Suite for Education users in primary and secondary (K-12) schools, Google does not collect or use any user personal information (or any information associated with a G Suite for Education Account) for advertising purposes or to create advertising profiles, whether in core services or other google services accessed while using a G Suite for Education account.

However, parents and educators should be aware Google may serve ads to G Suite for Education users in the "additional services," but administrators have the ability to restrict access to those additional services. Lastly, Google's terms state they do not assume ownership of any user data in the G Suite core services, and do not share or sell users' G Suite data to third parties.

Password Policy Best Practices for Strong Security

10 tips for stronger passwords Here's how to craft stronger passwords that will help stave off malicious actors on the web:

1- Never use the same password for multiple accounts.

2- Don't use personally identifiable terms.

3- Avoid using common words or phrases.

4- Use different types of characters.

5- Make it long.

6- Consider spelling things wrong.

7- Utilize multi-factor authentication.

8- Change your passwords regularly.

9- Never save or share passwords.

10- Use storage alphabet and number and symbol and others

Password complexity and length

Many organizations require passwords to include a variety of symbols, such as at least one number, both uppercase and lowercase letters, and one or more special characters. However, the benefit of these rules is not nearly as significant as expected, and they make passwords much harder for users to remember and type.

Password length, on the other hand, has been found to be a primary factor in password strength. Accordingly, encouraging users to choose long passwords or passphrases of up to 64 characters (including spaces).

Password age

recommended forcing users to change passwords every 90 days (180 days for passphrases). However, changing passwords too often irritates users and usually makes them reuse old passwords or use simple patterns, which hurts your information security posture. While strategies to prevent password reuse can be implemented, users will still find creative ways around them.

Therefore, the recommendation on maximum password age is to ask employees to create a new password only in the case of a potential threat or suspected unauthorized access.

Create a strong password & a more secure account

A secure password and updated recovery info help protect your Google Account.

Step 1: Create a strong password

A strong password helps you:

- Keep your personal info safe
- Protect your emails, files, and other content
- Prevent someone else from getting in to your account

Meet password requirements

Create your password using 12 characters or more. It can be any combination of letters, numbers, and symbols (ASCII-standard characters only). Accents and accented characters aren't supported.

You can't use a password that:

- Is particularly weak. Example: "password123"
- You've used before on your account
- Starts or ends with a blank space

Step 2: Be prepared if someone gets your password

Your recovery info is used to help you in case we detect unusual activity in your account.

Add a recovery email address

1. Go to your Google Account.
2. On the left navigation panel, click **Personal info**.
3. On the *Contact info* panel, click **Email**.
4. Click **Add Recovery Email**.

Add a recovery phone number

1. Go to your Google Account.
2. On the left navigation panel, click **Personal info**.
3. On the *Contact info* panel, click **Phone**.
4. Click **Add Recovery Phone**.

Recovery info can be used to help you:

- Find out if someone else is using your account
- Take back your account if someone else knows your password
- Get in to your account if you forget your password or can't sign in for another reason

Passwords especially susceptible to brute force attacks

- It's wise to use discourage or prohibit the following passwords:
- Easy-to-guess passwords, especially the phrase "password"
- A string of numbers or letters like "1234" or "abcd"
- A string of characters appearing sequentially on the keyboard, like "@#$%^&"
- A user's given name, the name of a spouse or partner, or other names
- The user's phone number or license plate number, anybody's birth date, or other information easily obtained about a user (e.g., address or alma mater)
- The same character typed multiple times like "zzzzzz"
- Words that can be found in a dictionary
- Default or suggested passwords, even if they seem strong
- Usernames or host names used as passwords
- Passwords that form pattern by incrementing a number or character at the beginning or end

User education

In addition, be sure to educate your users about the following:

- It is vital to remember your password without writing it down somewhere, so choose a strong password or passphrase that you will easily remember. If you have a lot of different passwords, you can use password management tools, but you must choose a strong master key and remember it.

- Be aware of how passwords are sent across the Internet. URLs (web addresses) that begin with “https://” rather than “http://” are more likely to be secure for use of your password.
- If you suspect that someone else may know your current password, change it immediately.
- Don't type your password while anyone is watching.
- Avoid using the same password for multiple websites containing sensitive information.