GOOGLE SHARED DRIVE, GOOGLE FORMS, AND GOOGLE SHEETS SECURE CONFIGURATION RECOMMENDATION

OVERVIEW

This document goes over the general security recommendations for creating and securing Google Shared Drive, Google Forms, and Google Sheets.

What is Google Shared Drive?

Google Drive and Google Shared drive are a cloud-based file storage and synchronization service. It allows you to store files in the cloud and share files with others easily.

Google Drive and Google Shared drive is also an office suite, which includes Google Docs (word processing), Google Sheets (spreadsheets), Slides (slideshow presentations), and more. You can collaborate with others to edit Google Docs, Sheets, and Slides concurrently.

You can use **Google Shared drives** in Google Drive to store, search, and access files with a team. Shared drive files belong to the team instead of an individual. Even if members leave, the files stay in place so your team can keep sharing information and work anywhere, from any device.

Can I store Protected Level 1(PL1) data in Google Drive?

Yes, Protected Level 1 data can be stored in Google Drive. However, secure Google Drive settings to store PL1 data **must** be implemented.

For HIPAA data, other requirements need to be in place. Please contact security@sdsu.edu to discuss your needs (to understand Protected Level 1 data please visit the CSU classification Data standard).

What is the process for storing PL 1 on Google Drive?

1. Start with planning what data needs to be stored, who should have access, and how it will be stored in Google.
2. Create a Google Shared Drive for each type of data and group according to step 1.
3. Apply the correct settings for Google drives
4. Use this document to record the settings and the names of who has access (treat this document as PL1 data)
5. Keep a copy of the document and share it with security@sdsu.edu.

What are the recommended secure settings for Google Shared Drive?

1. **NEVER** use a Google personal account to store SDSU data.
2. Always use the "**Least Access**" principle - Authorization to access data must be granted to individuals and must be restricted to only the data for which the individual has a need.
3. Annual HIPAA training is required for users with access to this classification of data.
4. Google Share Drive Configuration:
    - PHI Data and De-identified Data must be stored in two separate Google Share Drives
    - Microsoft Office Files containing PHI Data must also be encrypted prior to being stored in Google Share Drives
    - Encryption Keys/Passwords can not be stored on the same Google Share Drive as the files they are for. Encryption Keys/Passwords should be stored in a password manager like LastPass.
5. Multi-Factor Authentication must be enabled for any G Suite Account storing and accessing PHI Data.
6. User access to Google Share Drives must be documented and reviewed on a quarterly basis.
7. Google Drive App access must be reviewed on a quarterly basis
8. Never enable offline mode (PHI files should not be stored locally)
9. If using Google File stream (do not enable offline, laptop or workstations must be encrypted and joined the ID domain/Intune)

ADDITIONAL REFERENCES

- **ITUS Best Practices for Google Workspace**

Part 1a. Google Shared Drives General Security Recommendations

Google Drive allows you to share files with other users both within SDSU and even to external users outside of SDSU. It is critical to know what the options for access are available. These are the types of access options to choose from:

- **Public on the web** - Anyone on the Internet can find and access. No sign-in required.
- **Anyone with the link** - Anyone who has the link can access. No sign-in required.
- **SDSU University** - People at SDSU University can find and access.
- **People at SDSU with the link** - People at SDSU who have the link can access.
- **Private** - Only people explicitly granted permission can access. Sign-in required.

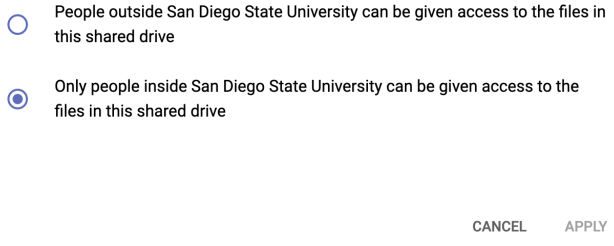
In addition, Google Drive allows you to assign permissions to specific users. These are the types of permissions to choose from:

- **Viewer.** People can view, but can't change or share the file with others.
- **Commenter.** People can make comments and suggestions, but can't change or share the file with others.
- **Editor.** People can make changes, accept or reject suggestions, and share the file with others.

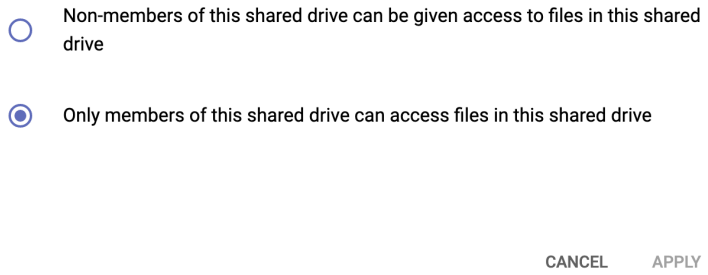
As a general security recommendation, it is best to practice the Principle of Least Privilege. Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.

1. You can set who has access to your Google Shared Drive.

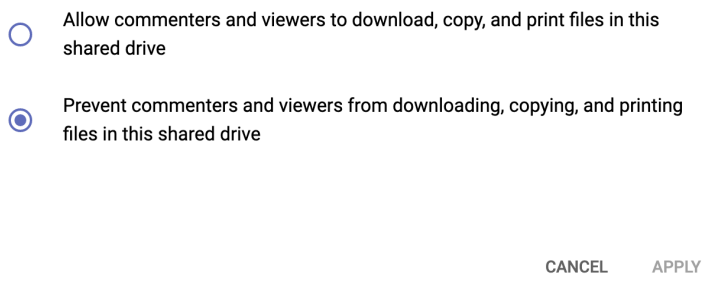
    a. ***Only people inside San Diego State University can be given access to the files in this shared drive.***



b. Only members of this shared drive can access files in this shared drive.

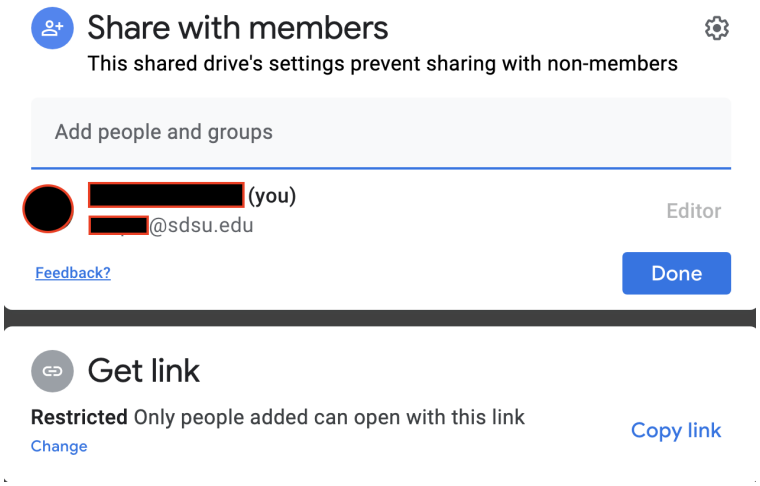


c. Prevent commenters and viewers from downloading, copying, and printing files in this shared drive.

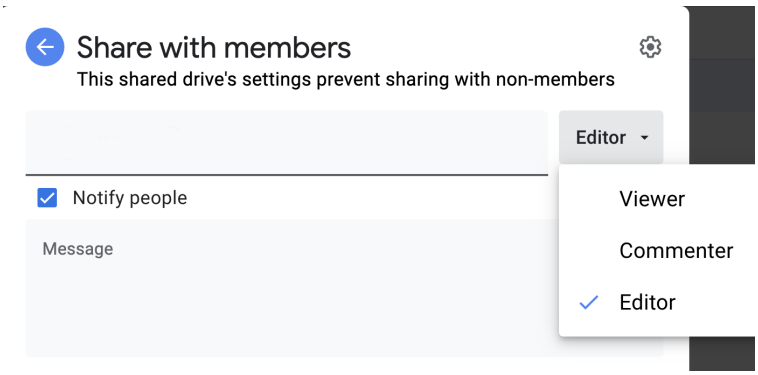


2. You can assign permissions to specific members:

a. Restricted Only people added can open with this link.



b. Always select the appropriate permission level[1].

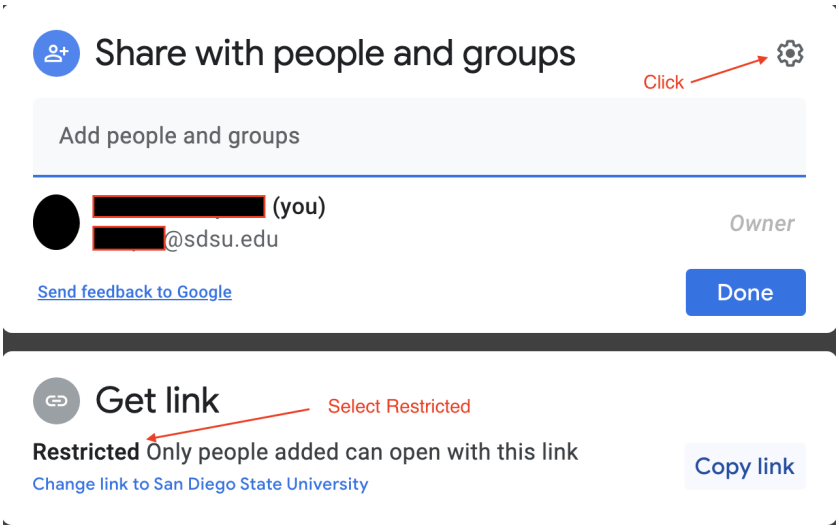


[1]From Google Sharing Settings Overview

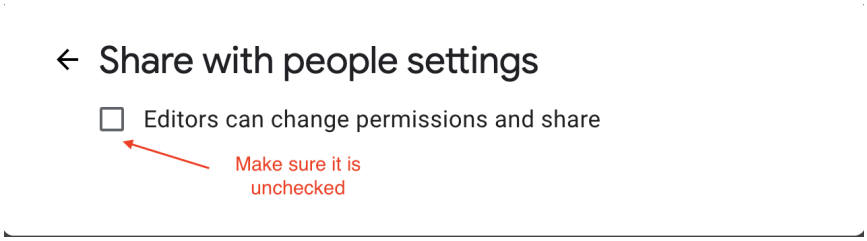
- **Viewer**: People can view, but can't change or share the file with others.
- **Commenter**: People can make comments and suggestions, but can't change or share the file with others.
- **Editor**: People can make changes, accept or reject suggestions, and share the file with others.

Part 1b. Google My Drive General Security Recommendations

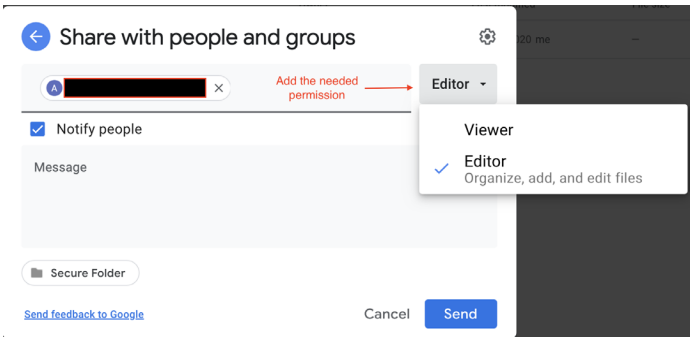
a. Create a Folder and apply these settings.



b. After clicking the cog ⚙ ***apply these setting.***



c. When sharing the folder, apply these settings.



Part 1c. Additional Information on Google Drive

1. Features

- Files remain after an employee leaves.
- All members of Shared drives see the same content.
- When a user is added to a Google group, they are automatically added to all of the Shared drives that include that group.
- You can add external users to a Shared drive.
- Files are searchable.

2. Technical Specifications

- Storage space
  - You can upload 750 GB of data per day.
  - You can upload files up to 5 TB in size.
  - If a single file exceeds the 750 GB daily limit, that file will upload. Subsequent files will not upload until the daily upload limit resets the next day.

- A Shared drive can contain a maximum of 250,000 files and folders.
- A Shared drive can include a large number of individual and Google Group members.
  - Limit for individuals and groups directly added as members: 600
    A group and an individual are both counted as one member against the limit.
  - Total limit of individuals (direct members, or indirect members due to Google Group membership): 50,000
    An individual who is a member of several groups that are added as direct members of the Shared drives still only count as a single individual.

- A single Shared drive can nest up to 20 subfolders, but we don't recommend creating Shared drives with a folder structure that complex. Shared drives function, but users can have difficulty organizing and navigating the content. Instead of a complex hierarchy of folders, consider organizing content into multiple Shared drives.

3. Data Security on Google Shared Drive

- Google Shared drives can be used to store up to PL1 Data as defined by the IT Security Office.
- Google Drive security uses TLS with 256-bit AES keys to encrypt data in transit.
- Data at rest on Google Share Drives are encrypted with 128-bit AES keys.
- If external documents are used, like Microsoft Word and Excel, an additional layer of encryption can be added to the documents by adding a password or setting which SDSU users can access the document.

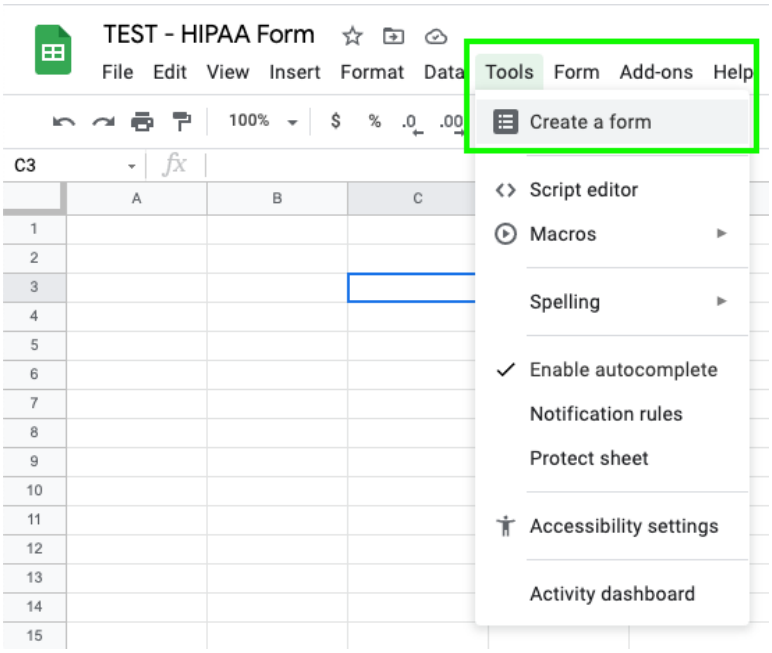
Part 2. Google Forms General Security Recommendations

You may also use Google Forms to collect PL1 Data as long as the following recommendations are followed.

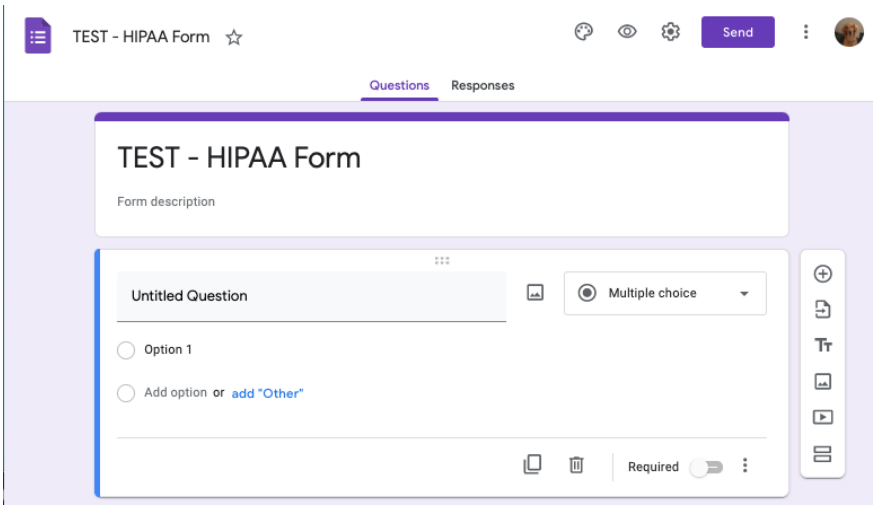
- Whenever possible, collect Subject information using a Subject ID rather than any identifying information like First Name Last Name. This helps to de-identify the data and reduce the data security risk in case any of the data is compromised.
- Make sure that only the authorized users have access to the Google Sheet Data.
- If you plan to use any "add-ons", you must verify with ITSO if they can be used in compliance with PL1 Data.
- It is recommended that emails should be sent directly to human subjects so that only the specified user receives the link for the survey.

Creating a Google From that collects PL1 Data requires the following:

1. You must make sure to create the Google Sheet first in your PL1 Google Share Drive.
    a. Do not create the Form first as the Google Sheet created may not reside in your PL1 Google ShareDrive.
2. Please name your spreadsheet.
3. To create the Google Form, click on "Tools > Create a form."



4. A new tab will open where you can begin to build your Google form.

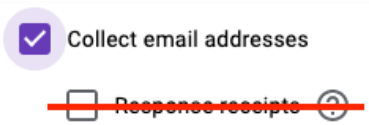


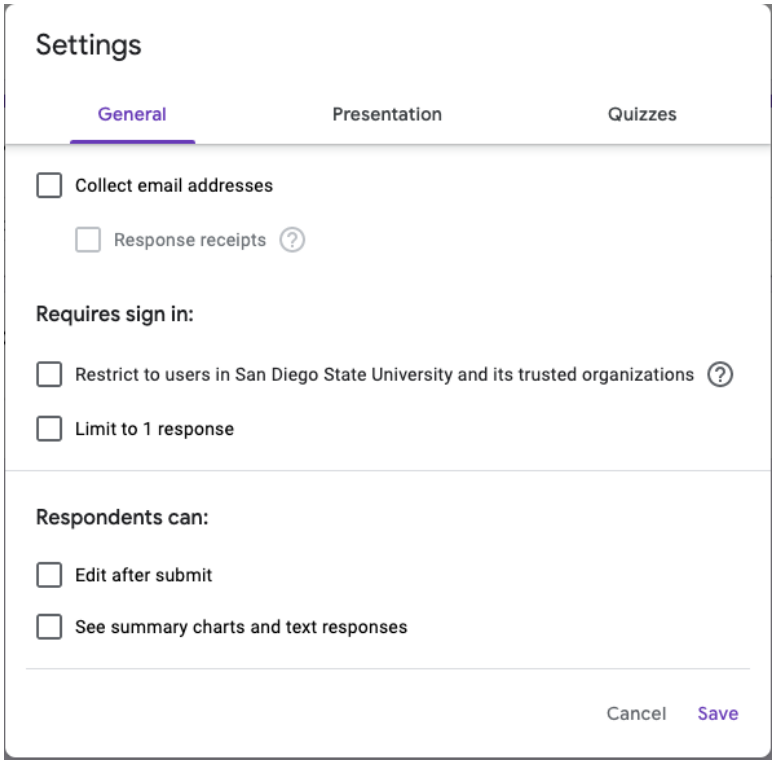
Google Form Settings

a. Select the "cog" icon in the top right corner.

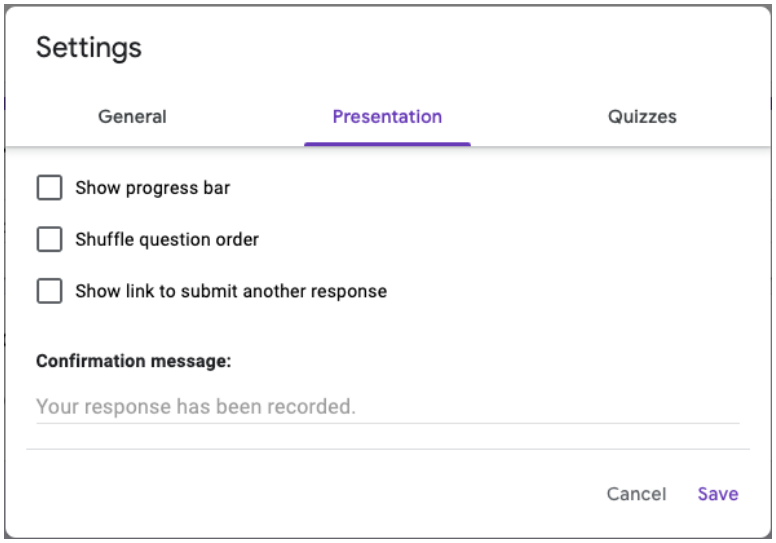
b. On the first tab "General", select the appropriate settings for your survey.

a. If you choose the option "Collect email addresses", **do not** select "Response Receipts". This option sends the user a copy of their responses and, therefore, could violate certain privacy rules depending on where the copy is received.

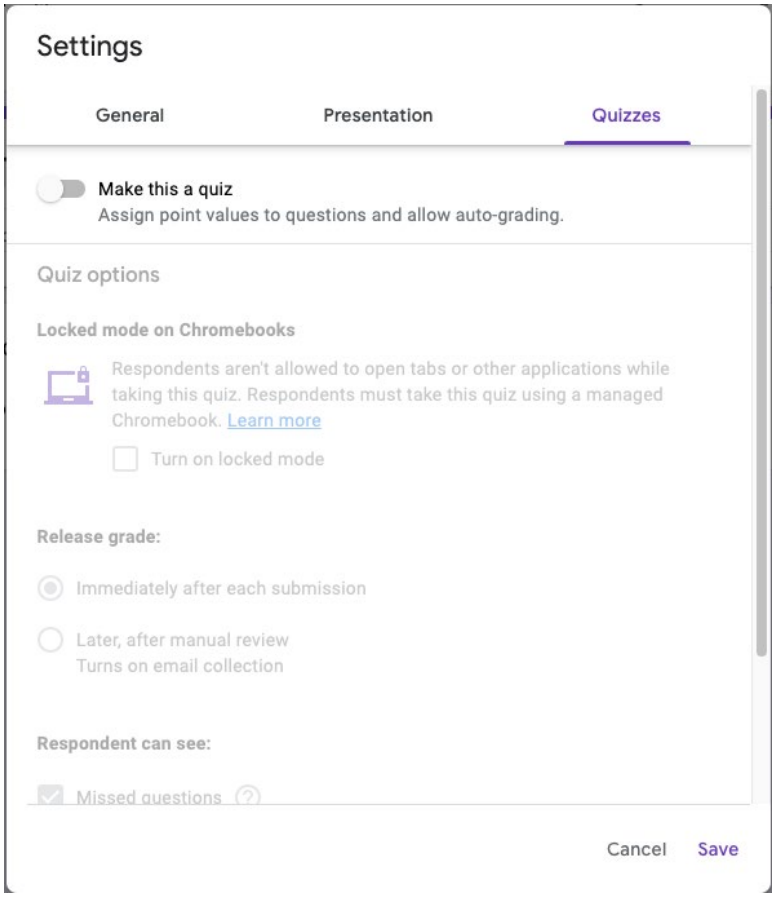




c. On the second tab "Presentation", select the appropriate settings for your survey.

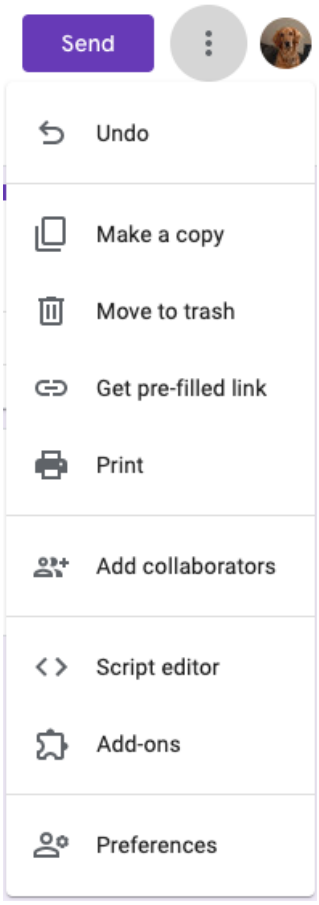


d. On the third tab "Quizzes", there should be no changes needed.



e. Additional information on sending the Google Form can be found here:
https://support.google.com/docs/answer/2839588

Note: The above article also covers how to send pre-filled forms/surveys to users. This may be a beneficial option if you are using Subject ID numbers to track user information.

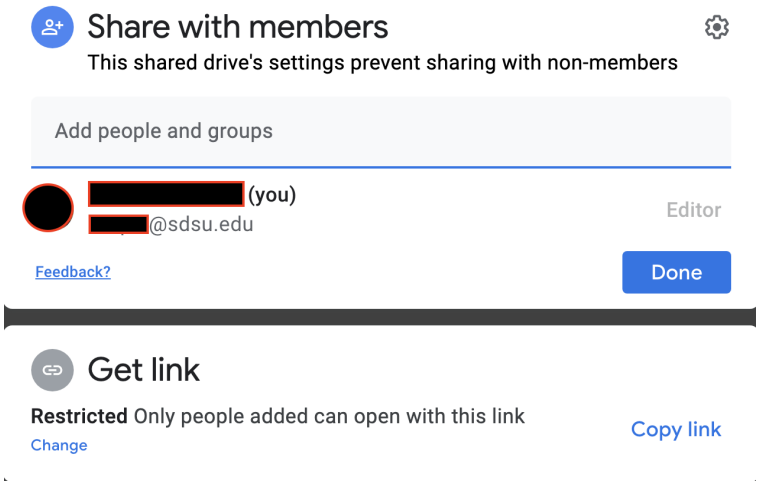

Send
Undo
Make a copy
Move to trash
Get pre-filled link
Print
Add collaborators
Script editor
Add-ons
Preferences

Part 3. Google Sheets General Security Recommendations

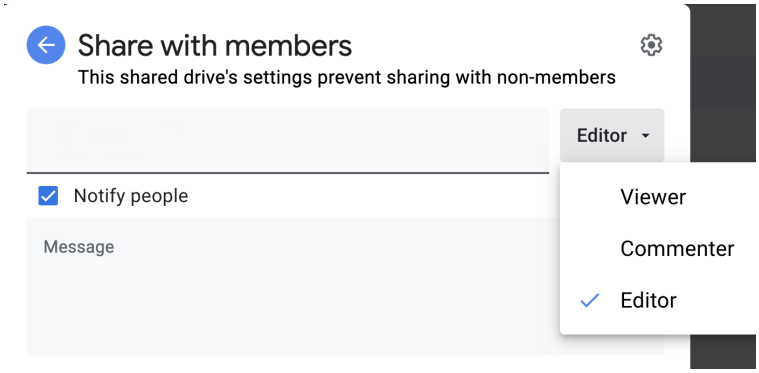
Protect individual worksheets in a Google Spreadsheet. Similar to a Google Doc, users have the option to set permissions that will give editing rights to: anyone invited as a collaborator; only you; or a list of collaborators. The following gives you general security recommendations on how to secure your Google Sheet.

1. When sharing files, make sure these settings are selected:

    a. ***Restricted Only people added can open with this link.***



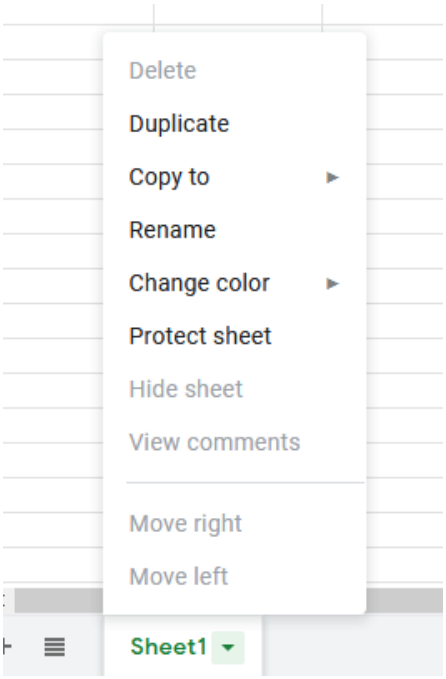
b. Always select the appropriate permission level[2].

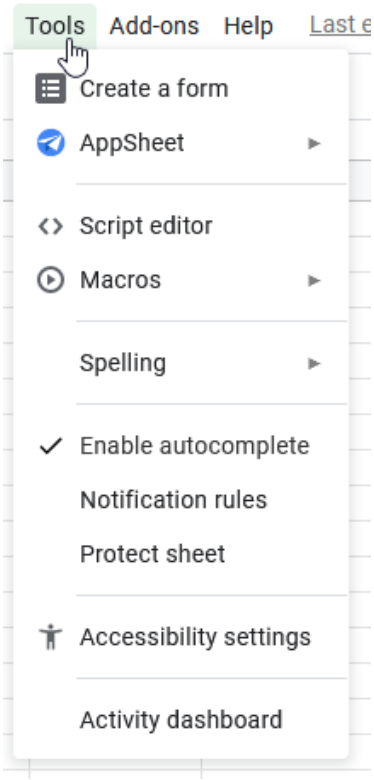


2. If you don't want people to change the content in a spreadsheet, you can protect it. Keep in mind that people can print, copy, paste, and import and export copies of a protected spreadsheet. Only share spreadsheets with people you trust.

a. Select a tab and right click. Then, select "Protect sheet." You can also select "Tools" from the menu and choose "Protect sheet."

[2]From Google Sharing Settings Overview
- **Viewer**: People can view, but can't change or share the file with others.
- **Commenter**: People can make comments and suggestions, but can't change or share the file with others.
- **Editor**: People can make changes, accept or reject suggestions, and share the file with others.

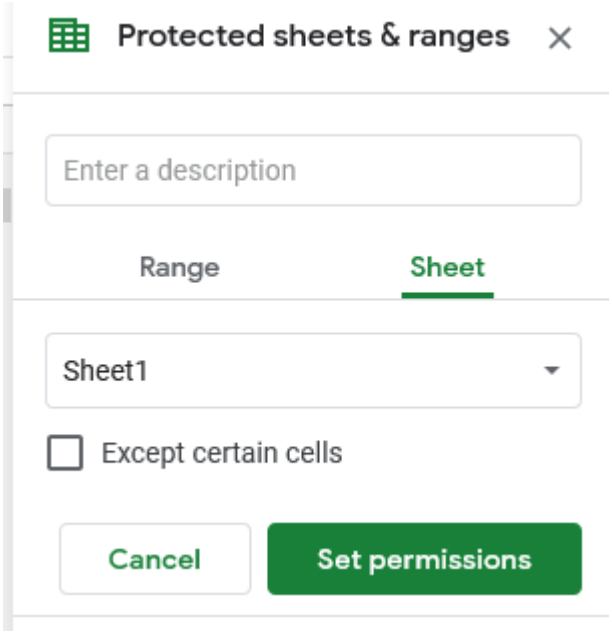

Delete
Duplicate
Copy to
Rename
Change color
Protect sheet
Hide sheet
View comments
Move right
Move left
Sheet1


Tools
Add-ons
Help
Last e
Create a form
AppSheet
Script editor
Macros
Spelling
Enable autocomplete
Notification rules
Protect sheet
Accessibility settings
Activity dashboard

b. To protect a range or a sheet, click Add a sheet or range or click an existing protection to edit it. To protect a range, click Range. To protect a sheet, click Sheet.

- *Range*: To change or enter the range you're protecting, click the spreadsheet icon and highlight the range in the spreadsheet.

- *Sheet*: Choose a sheet to protect. If you want a set of cells to be unprotected in a sheet, check the box next to "Except certain cells."



c. "Set permissions" allows users to restrict who has access to a range or a sheet.

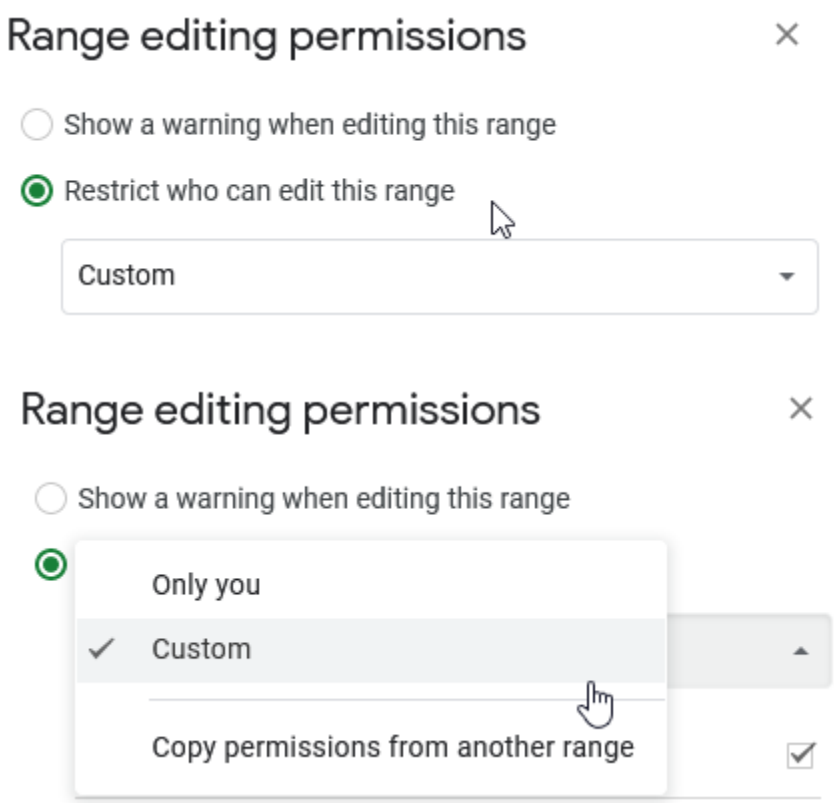
- Choose how you want to limit editing:

  - *To show a warning when anyone makes an edit*: Select "Show a warning when editing this range." It doesn't block people from editing, but they'll see a message asking them to confirm if they really want to make an edit.

  - *To choose who can edit the range or sheet*: Select "Restrict who can edit this range." Choose:
    - *Only you*: Only you (and the owner if you're not the owner) can edit the range or sheet.

- *Only domain*: If you use Google Sheets for work or school, only people in your domain can edit the range or sheet. This option is only available when everyone in your domain can edit the spreadsheet.
- *Custom*: Only the people you choose can edit the range or sheet.
- *Copy permissions from another range*: Reuse the same permissions you set up on a different set of cells or sheets.

- Click **Save** or **Done** when you have set your permissions.



d. Note who can protect a range or a sheet:

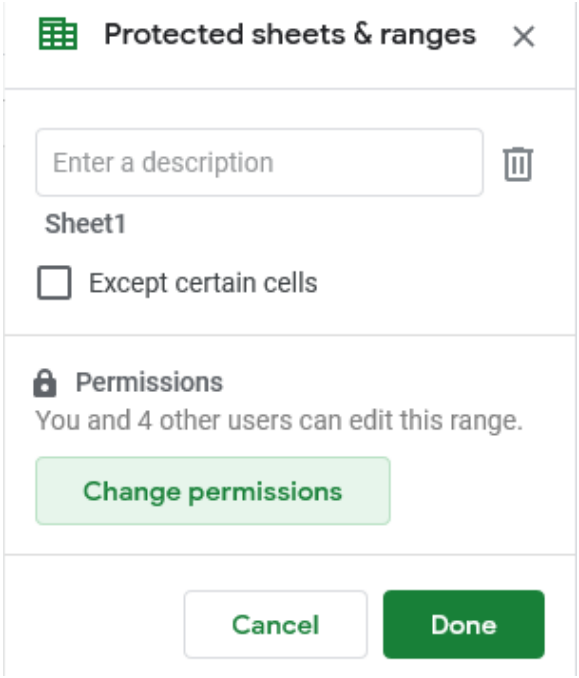
- *If you own a spreadsheet:* You can decide who can change ranges and sheets.
- *If you can edit a spreadsheet:* You can decide who can edit ranges and sheets but cannot take permissions away from owners.
- *If you can view or comment on a spreadsheet:* You will not be able to make any changes.

e. Note who can edit a copy of a protected range or a sheet:

- *If you can edit:* You can make a copy of the protected sheet, copy the workbook, or upload a new version.
- *If you can view but not edit:* You can make a copy of the spreadsheet.

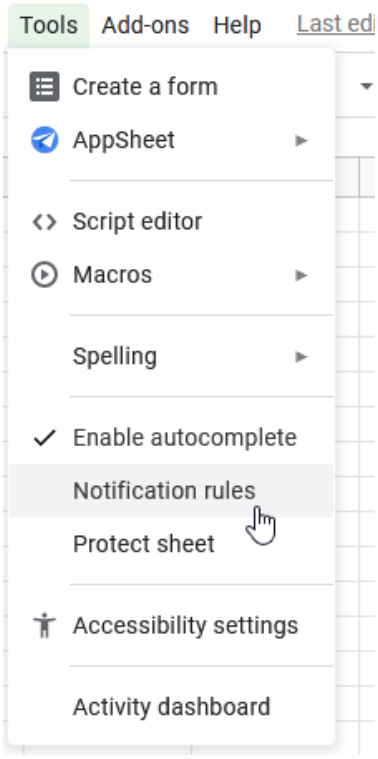
f. Note how to remove protection of a range or a sheet:

- In a Google Sheet, click Data > Protect Sheets and ranges.
- On the right panel that appears, to view all of the ranges with protections, click Cancel.
- Find protection you want to delete > Click delete .

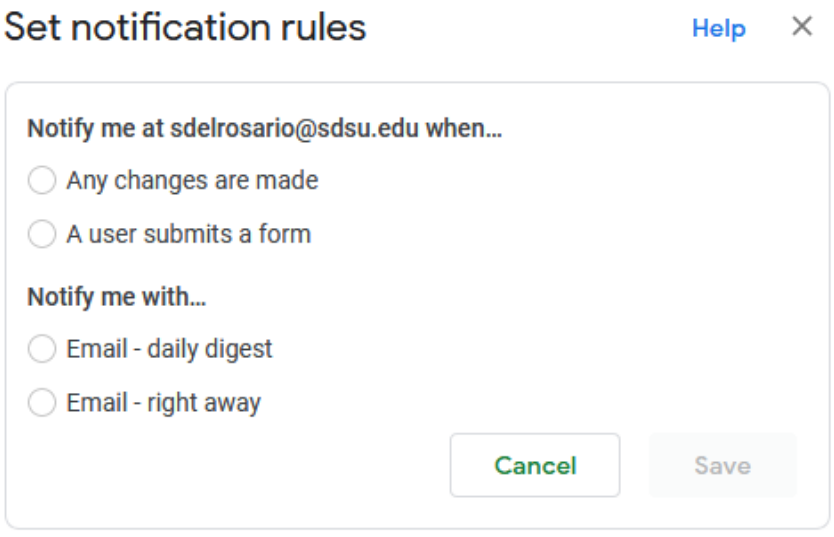


3. Get notified of any changes in a Google Spreadsheet by setting up notification rules.

a. To do this, select "Tools" from the menu and choose "Notification rules."

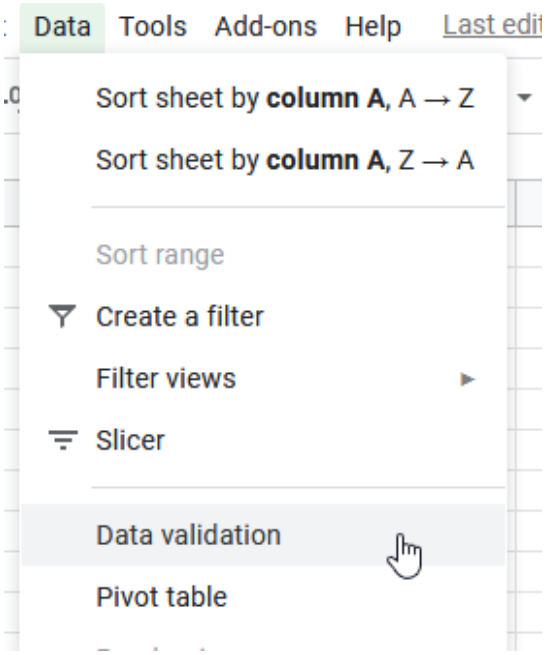


b. ***Set the Notification rules.*** *You have the option to be notified when changes are made to: the spreadsheet; a specific worksheet; a cell or cell range; collaborators; or (if the spreadsheet is joined to a form) when a user submits a form. Notifications can be sent as soon as a change is made or as a daily summary.*



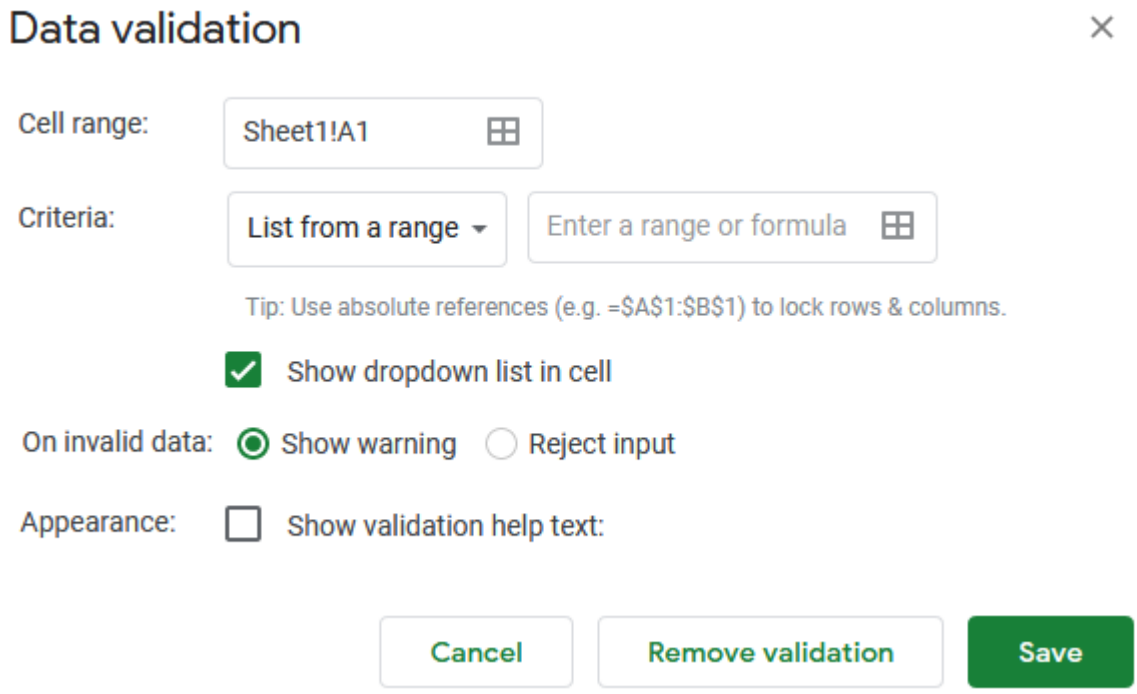
4. Set Data Validation rules to stop individual cells or a range or cells from being edited by setting a value that the cell must have.

    a. ***To do this, select "Data" from the menu and choose "Data Validation."***



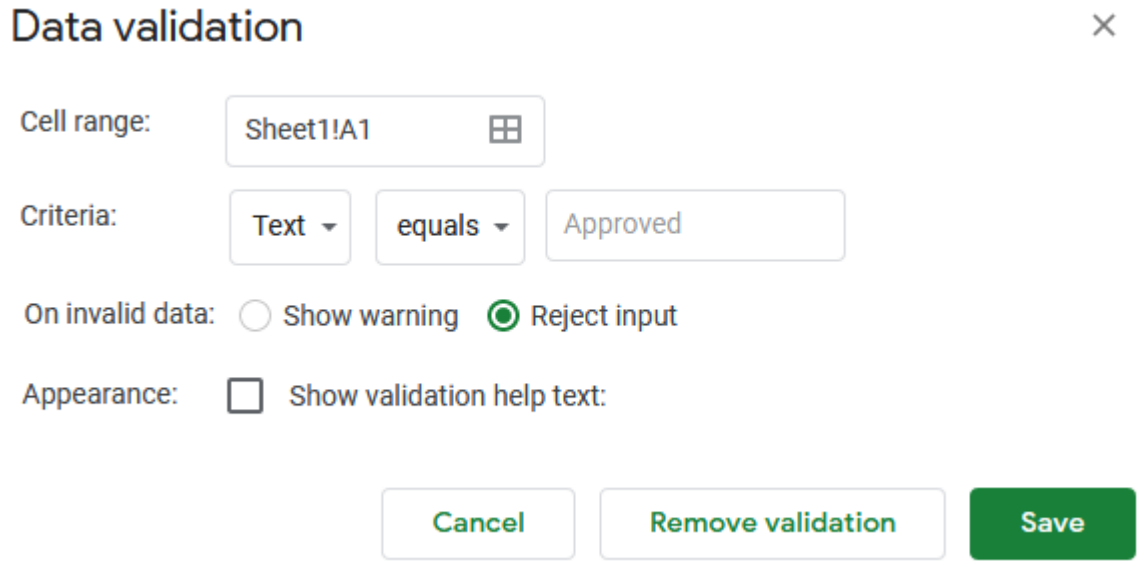
b. ***Choose to set a Number, Text, Date or Items from a List.*** *Each criteria has further settings, for example: a Number cell can be a range or maximum value; a Text cell can be set to contain or not contain word(s); a Date cell can be set to be a valid date only; and a List cell can only be populated from a list.*

A further option enables you to either warn the editor that validation rules have not been met but allow the change ("Show warning'), or disallow any changes that do not meet the criteria ("Reject input).



c. ***Protect cells with formulas.*** *Data validation is a very useful method to ensure that cells containing a formula are not mistakenly edited. To do this:*

- *Select the cell or range you want to be validated.*
- *Select the Text criteria and set the second drop down to "equals."*
- *In the blank box add your cell formula.*
- *Select "Reject input" on invalid data..*



Revision History

Date	Author	Version	Description
July 2021	SDR	1	