Data Protection is ***People*** *Protection*

MERCY CORPS

DATA PROTECTION & PRIVACY GUIDE:

File Sharing Best Practices

This guide covers file sharing best practices for Mercy Corps team members using G Suite apps, particularly Google My Drive. To simplify this guide, we will be discussing sharing a single *file*, such as a spreadsheet. However, the same options are available when sharing a My Drive *folder*.

Note: Mercy Corps is transitioning to Microsoft 365 for file sharing. Once best practices for that platform have been established, a similar document or resource will be created.

☆ Importance

There are several reasons why it is better to share a file by hosting it in Google Drive and sending a link rather than as an attachment in an email.

- **Security:** you can easily change who is permitted to access or edit your file. You can also make the link time sensitive by only allowing access to the file for a given period of time.
- **Version control:** when sharing a file that is hosted online, many people can access it at once and all changes and comments will stay in one file. Sending a file as an attachment often results in multiple versions of the same document with different file names, edits, comments, etc. The document owner will spend a lot of time trying to compile all of this into a single file! Using a link also guarantees that the recipients always have access to the most updated version of the document.
- **File sizes:** Some IT departments impose restrictions on the size of attachment that are allowed. Sending a link allows you to share files of any size.
- **Easy editing:** Files shared as Google documents in Drive, Microsoft Word in OneDrive, or similar formats allow the recipient to open and interact with the document using a web browser: they do not have to have the most recent version of a particular type of software.

Principles

Whenever you share documents, you should consider the following:

- **Carefully consider who will create the file or folder, who will own/administer it, and who will access it. If short-term contractors create and administer files there is a risk of the files or the access leaving with the contractors when they leave!**
  - Only give access to those who need the file.
  - Confidential, private or personally identifiable information (PII) content must *always* have restricted access. If you are unable to determine if or how the content should be restricted, please seek assistance from Legal or the Data Protection and Privacy team.
- **Use the appropriate level of permissions.**
  - Consider an example where a new project charter needs to be created. Most likely, only the team responsible for charter creation should have full access. When it's time to get feedback from others, grant additional permissions that only allow viewing or commenting.
  - Use extreme caution in granting access requests to team members who may accidentally be using their personal email accounts. Instead of granting access to a personal email account, grant access to their Mercy Corps account, and ask the team member to log in with those credentials.
- **Permissions change over time.**
  - If you are only working with someone for a short period of time or with people outside Mercy Corps, consider giving temporary permissions. If you forget to remove the access later, an expiration date will ensure their access is suspended at the right time.
  - Periodically audit the list of who has access to your files, folders or shared drives to ensure you remove access for team members who have changed roles, or are no longer with Mercy Corps.

› Risky content requires extra steps.

- Personally identifiable information (PII), demographically identifiable information (DII), or other types of personal data are protected under multiple data protection laws. Before you share personal data, verify the legal requirements for sharing that information with others. Inappropriate personal data sharing can put program participants, donors, partners and Mercy Corps team members at risk. If you have questions about personal data or data protection laws, please email the Data Protection and Privacy team at dataprotection@mercycorps.org.
- If the information is considered confidential or proprietary for business purposes, share it only with required parties and consider granting temporary access.
- If the person receiving the file works in an insecure location, or if the contents include personal data, consider encrypting the file or protecting it with password protection. See the Encryption and de-identification sections for examples of how to do this.

› Never move files without the owner's permission.

- Moving files may alter who has access and make it impossible for others to find the file! Always check with the document owner before moving a shared file to a new location.

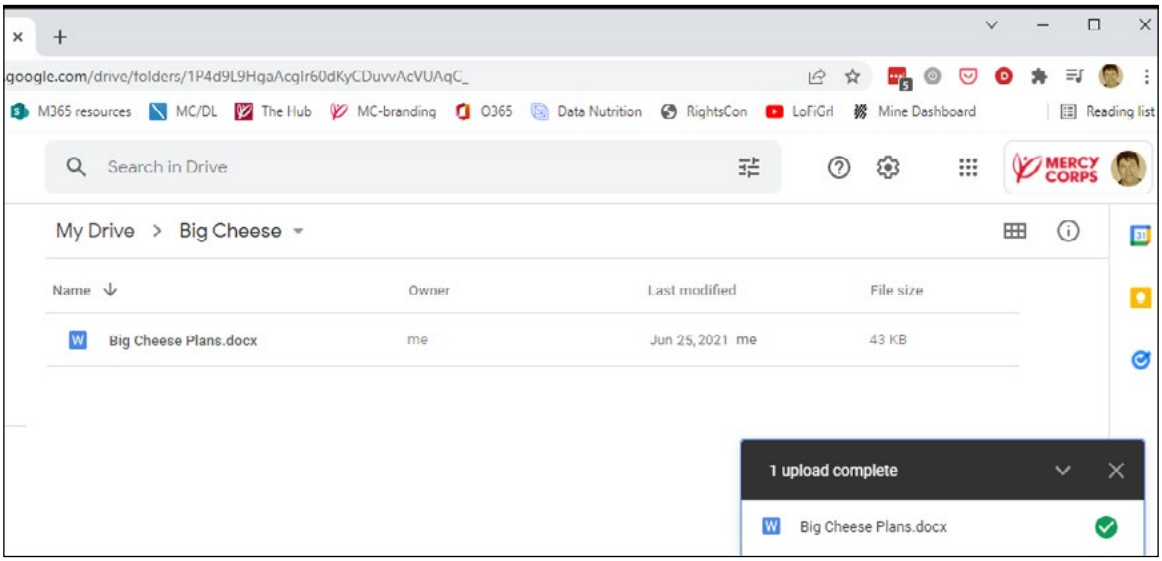
File Sharing: GDrive

Here is a sample use-case for sharing a file using best practices in Google Drive. Imagine that the year is 2020 and Mercy Corps is working with a consultant (PNW Rocks), to create materials for a major new initiative at Mercy Corps, that is code-named Big Cheese. The Big Cheese project will not be announced publicly until July 2021 so it's important to limit who has access to the file. To get started, we'll want to collaborate on next steps for the project in a file called "Big Cheese Plans."

Instructions

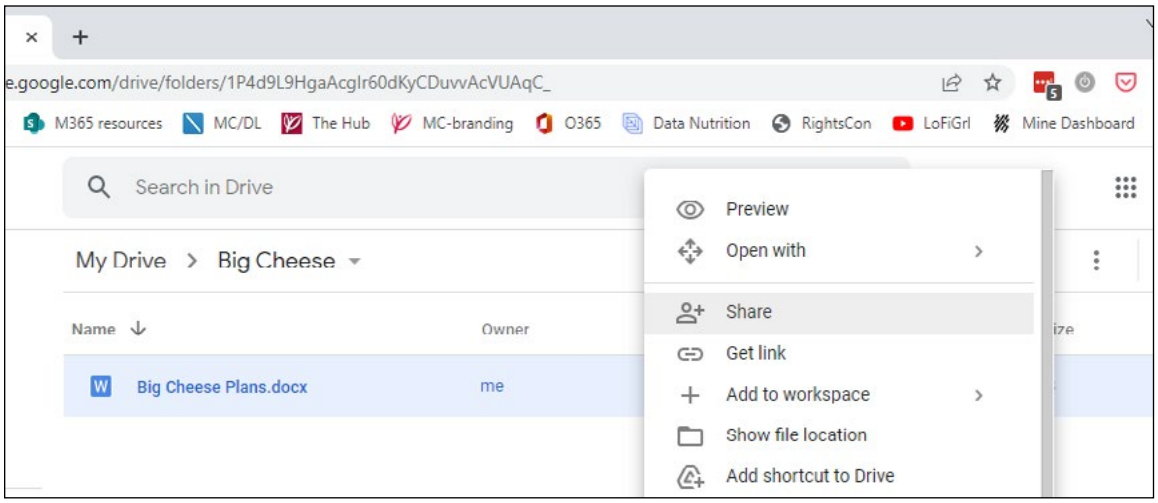
Step 1 - Upload

Upload the file to My Drive.



Step 2 - Share

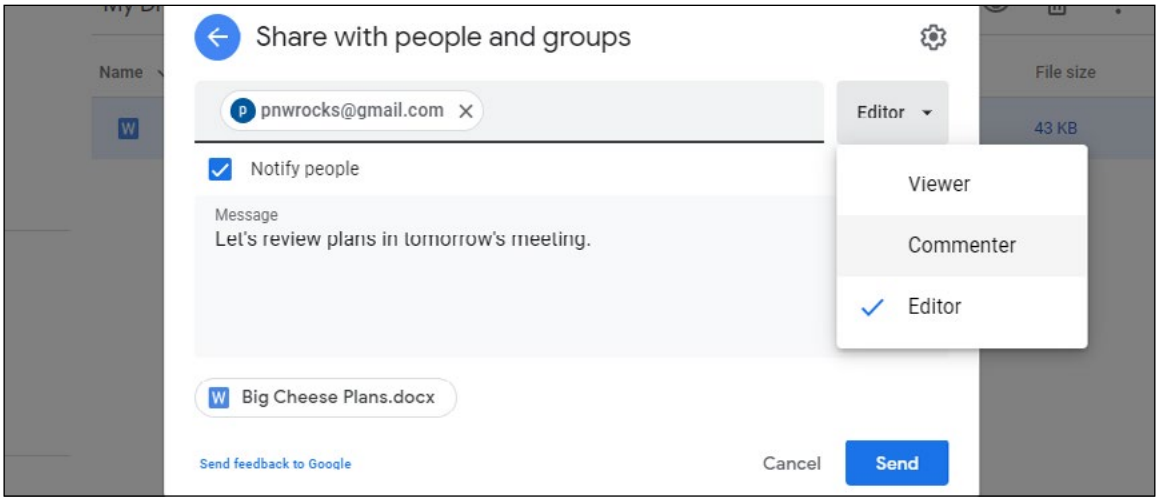
To share the file, right-click the file and then click **Share**.



- Only give access to those who need the file. When you share a file in My Drive, the default setting is **Restricted** (to persons or groups), which is the best practice. Remember, confidential, private or personally identifiable information (PII) content should *always* have restricted access!
- The **Anyone with the link** option should only be used for files that hold no confidential information and are open to the public. If the **Anyone with the link** setting is used on a file with confidential private, personal or financial data, it could easily and accidentally be shared and put Mercy Corps at immediate legal risk and make it easy for bad actors to use the information for criminal purposes.

Step 3 - Select level of access

Enter the email address for the person you want to share with, then choose the level of access. Google defaults to **Editor** access, which is only appropriate for team members who need full access to the document. When you are engaging stakeholders for feedback, choose **Viewer** or **Commenter**. Best practice is to notify the person, and add a message, explaining why you've shared the file. To notify, leave that **Notify people** box checked. When done with changes, click **Send**.

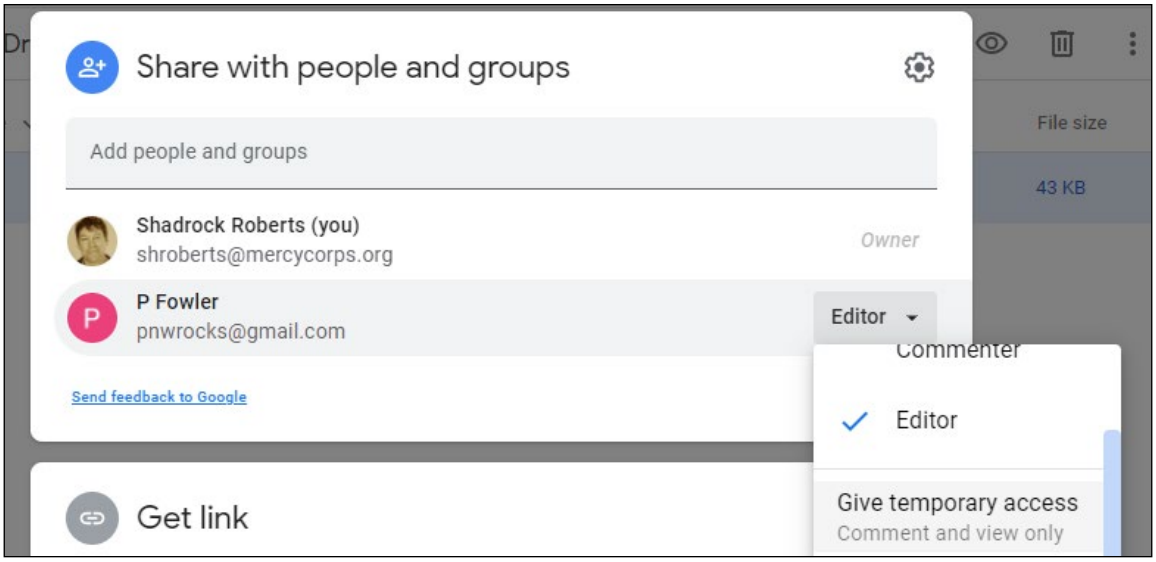


Another option is to send a separate email with a link to the file. To notify separately via email, uncheck the **Notify people** box. After clicking **Done**, right click the file and choose **Get Link**. In the new popup window, click the **Copy link** button, and then paste it into your email.

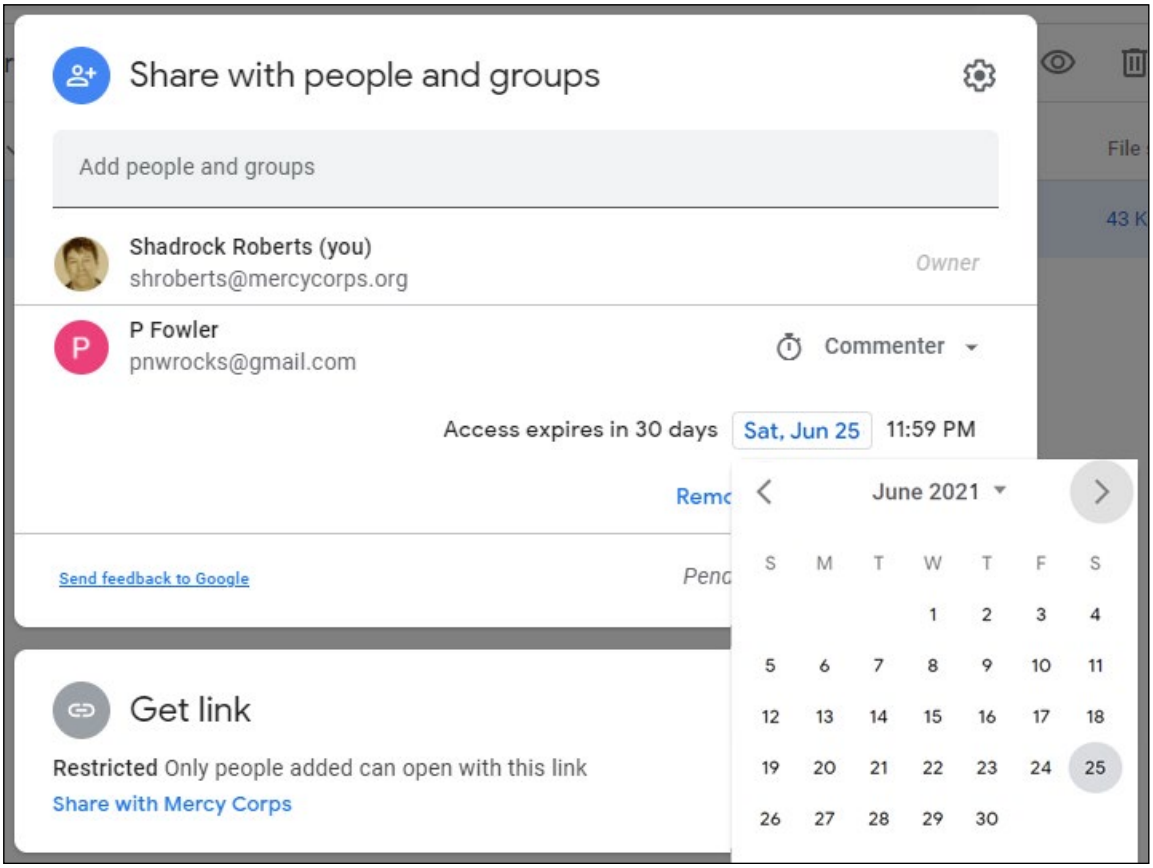
- To learn more about access levels, visit Share and collaborate in My Drive.
- If you restrict a file, and someone with access shares the link with another person, that person will not automatically have access to that content in Google Drive. Instead, they'll see a web page with the opportunity to request access. The request for access will go to the file owner. Access requests should be reviewed, and those receiving access requests should not simply grant permission to any and all requests, without reviewing the above notes and considerations.

Step 4 - Temporary Access

Once permission has been granted, the sharing time period can be shortened. To limit access, right click the file again, and click **Share**. Find the email address you just shared with and right click the access level. You will see new options appear; select **Give temporary access**.



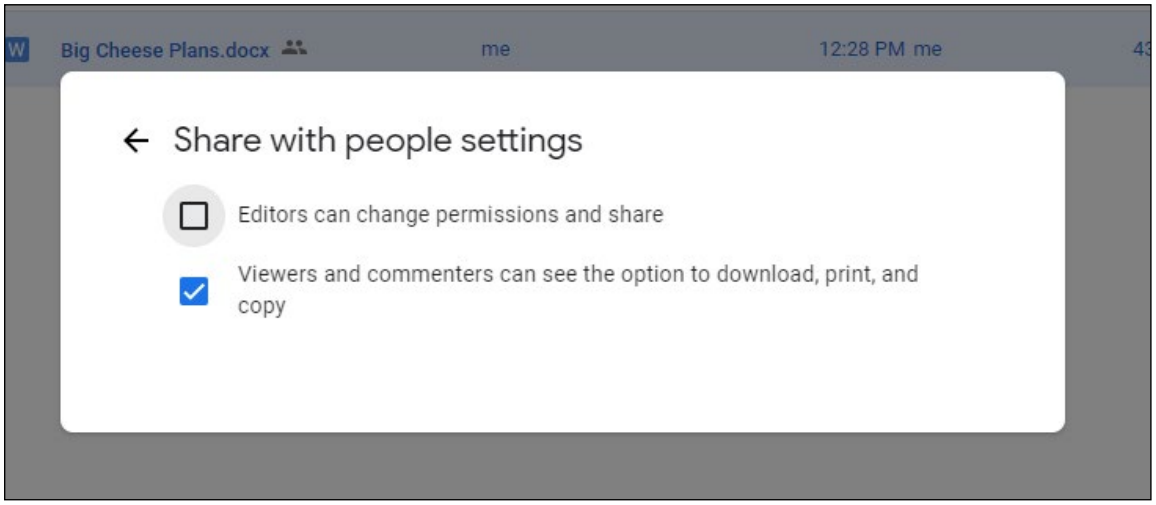
A calendar will appear. Navigate to the month when access should expire, and click the corresponding date.



The calendar will disappear, and the display date will change. Once you can see that access will expire on the correct date. Click **Save**.

Step 5 - Additional Options

If you have concerns about others taking inappropriate actions with the content, there are additional options available in the settings screen. File settings can be accessed from the gear icon in the upper right of the sharing window. Click the gear and you'll see options to restrict further sharing, or disabling the option to download, print or copy. For any feature you want to disable, simply uncheck the box. The file will quickly update, saving the new setting.



- To learn more, visit Restrict sharing options on Drive.

Additional considerations

- Do not place confidential files inside folders that are shared widely. Shared folders permissions trickle down to each file and subfolder, so your confidential file could be accessed by anyone with permission to the parent folder! Instead, move your confidential file to a new location, outside the larger shared folder structure.
- Once a file has been shared, you may have the option to **Make a Copy** and/or **Move** the file to another location. Never move a file without the owner's permission!
- If you need to see the file in your My Drive or in a secondary location, the best practice is to use the Add shortcut to Drive option.
- If a file copy is made, or the file is moved, be aware it will not have the same permissions as the original file unless you explicitly set those permissions.

This guide does not cover file sharing in Google's shared drives, nor external file sharing platforms. To learn more about these, visit Google's Best practices for shared drives or managing shared drives page. Each of these pages is available in a variety of languages: scroll to the bottom of the page to select your language.

The best way to control access to files using Drive is to create a Google group and assign permissions to those in the group. Google groups are not just for sending emails; groups are powerful and convenient tools for managing folder and file permissions. Find out more about Google Groups.

If your project requires the use of applications outside of G Suite, encourage your team to download Google Drive for desktop. This program allows you to view any documents in My Drive or Shared drives as if they were on your laptop, even when offline, and without having to download the item or convert it to a Google format.

Further Assistance

How and with whom you will share data should be part of a larger strategy for the data life cycle of a program or activity. There are several resources that can help you.

- The International Federation of Red Cross and Red Crescent Societies (IFRC) *Data Playbook* is an excellent resource of exercises, session plans, checklists, and other materials to help you organize conversations and activities with your team. In particular, Module 7 - Data Sharing is a good place to start.
- The International Committee of the Red Cross' *Handbook on Data Protection in Humanitarian Action* is a detailed guide to almost every aspect of humanitarian data. Chapter 2 specifically deals with data sharing.
- The Cash Learning Partnership's *Data Responsibility Toolkit* is designed for cash and voucher practitioners specifically, but is a "gold standard" in guidance for responsible data. See especially, *Tip Sheet #6, "Data Sharing"*. The Toolkit is available in English, Arabic, French, and Spanish.

CONTACT

HEATHER LOVE
Director, Global Data Protection and Privacy | IT
hlove@mercycorps.org

SHADROCK ROBERTS
Data Protection Specialist | IT
shroberts@mercycorps.org

About Mercy Corps
Mercy Corps is a leading global organization powered by the belief that a better world is possible. In disaster, in hardship, in more than 40 countries around the world, we partner to put bold solutions into action—helping people triumph over adversity and build stronger communities from within. Now, and for the future.

MERCY CORPS

Global Headquarters
45 SW Ankeny Street
Portland, Oregon 97204
888.842.0842
mercycorps.org

European Headquarters
40 Sciences
Edinburgh EH9 1NJ
Scotland, UK
+44.131.662.5160
mercycorps.org.uk