MONTCLAIR
STATE UNIVERSITY

Using Google Drive with Sensitive Data

A practical guide for protecting data/files collected, stored shared using Google Drive (Docs, Sheets, and Slides)

Office of the Chief Information Security Officer (CISO)
Information Security
Division of Information Technology
Montclair State University

Updated November, 2023

Overview

As part of its normal business and academic operations, Montclair State University collects, processes, and retains personal information and data related to prospective students, enrolled students, employees, affiliates, and others. The University has an obligation to protect any such information from unauthorized or unnecessary access. This type of information is classified as sensitive data. More information regarding sensitive data including examples by classification can be found in the University's Data Classification & Handling Policy.

Tip: In general, sensitive data is the type of data that you would not want others to know unless it was necessary and authorized. Examples include your social security number, credit card or bank account information, health information, government IDs, etc.

As related to various University business processes, sensitive data often needs to be collected, stored, and shared (distributed) for collaborative purposes. Electronic forms and report files are two examples.

The University utilizes the Google Workspace for Education service to support a variety of business needs: Gmail, Calendar, and Drive, along with Docs, Sheets, and Slides. Google Drive stores Docs, Sheets, and Slides files in their native Google format, as well as files from other applications such as Microsoft Word, Excel, and Powerpoint files that are uploaded to Google Drive.

When using Google Drive to collect, store, or share files that contain sensitive data, it is critically important that you take two key steps towards protecting the data:

I. Protect Your Account
II. Share with Care

I. Protect Your Account

These practices should be followed to reduce the risk of unauthorized access to your Google account:

1. Practice "good credential hygiene" and **ensure your NetID and other account passwords are:**
    a. **Strong**. Change your password if it contains any common phrases (e.g. "redhawk") or personal information references (e.g. "my pet's name that I post to

social media"). Consider using a *passphrase* which is typically composed of a string of words similar to a sentence. Remember that "longer is stronger" when it comes to password/passphrase composition.

b. **Unique**. Do not use the same password with **any other account.** Do not reuse a password that you have used previously (with any account).
c. **Private**. Do not share your password with anyone, ever. Do not write your password down where it can be discovered by others. Consider using a secure password manager app to store your passwords.

2. **Enable and always use Google's "2-Step Authentication" account security feature**

   (NOTE: As of Fall 2023, all employee and student accounts are required to use MFA to access the University's primary Google Workspace instance (@montclair.edu) through Single Sign-On (SSO)/NEST. However, if you are utilizing a special instance of Google Workspace or your personal Google account to do anything work related, you should enable 2-Step Authentication on that separate account.)

   This is a form of *multi-factor authentication* or "MFA" for short. For authentication purposes additional *factors* are, "something you know, something you have, or something you are". A password or PIN is an example of something you know and is the first factor. Adding a second factor such as something you have (i.e. a cell phone) makes it tremendously more difficult for someone else to authenticate as you and access your account.

   a. More information on Google's MFA implementation, called "2-Step Authentication", as well as instructions on how to enable it for your MSU Google account can be found here: https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome

---

Tip: While it does come with a small initial learning curve and an extra step when logging in to your account, **enabling Google 2-Step Authentication is the most practical and effective step you can take to protect your account against unauthorized access at this time.**

II. Share with Care

Access Control is the process by which a user is authorized to access data. In Google Drive, access control takes the form of file ownership and sharing.

File Ownership

You own any file that you initially create or upload to "My Drive", the default location for your Google Drive account. These files, by default, are initially only accessible to your account.

Sharing

To share access to a file, you must use the “Share” feature on a file or folder. **How you manage sharing is critically important for the protection of data on Google Drive.**

Documentation on Google Drive sharing can be found in the Google Workspace Learning Center:

- Share files from Google Drive
- Share folders from Google Drive

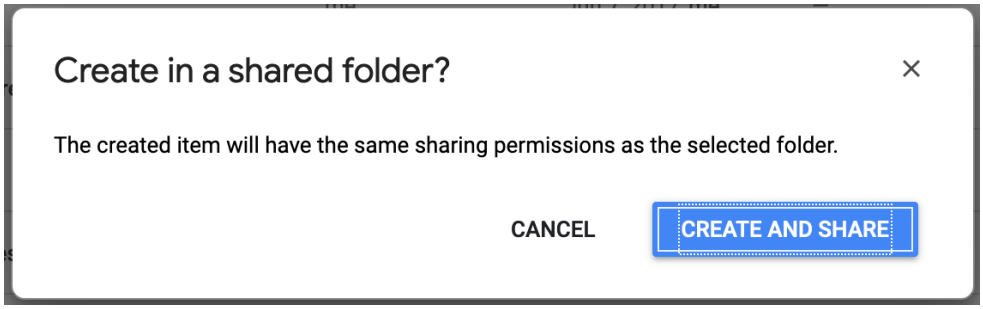
In general, when you share files or folders in Google Drive you want to consider the following:

1. **Follow the principle of “need to know”**. Use caution when sharing a file or folder. Only include recipients that are not only authorized but *need* to view the data in question. Sharing files with someone who *might* need the data only increases the risk of exposure as those recipients may not be as invested in or aware of the need to protect the information.

Tip: File vs. Folder sharing

While it may take a little more effort to manage sharing at the individual file level, doing so provides more granular access control then sharing at the folder level. If sharing by folder, be sure *all of the files* in the folder (and any sub-folders) are intended to be accessible by *everyone* you are sharing the folder with.

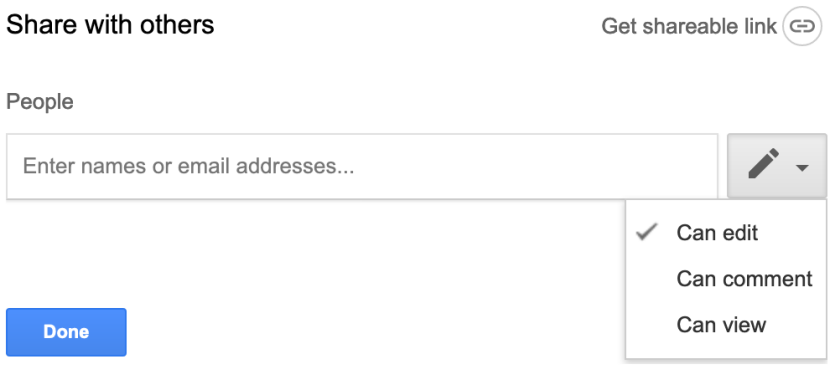
Also, be sure to pay attention to the permissions you are granting to the recipient(s) of a shared folder as these permissions *apply to all enclosed files and subfolders* unless overridden by an individual file or sub-folder’s own sharing permissions. (i.e. Granting “Can organize, add, & edit” will also grant full “Can edit” permission to all enclosed files in that folder that do not have individual sharing permissions set.)



---

2. **Follow the principle of “least privilege”**. Google file sharing includes three levels of permissions to be granted: Can Edit, Can Comment, Can View. Do not grant a higher level of permission than recipient(s) require. Consider the actual need of each individual recipient.

Tip: Be aware that the least restrictive option is at the **bottom** of the pull down menu list (see picture below). Therefore, adding recipient addresses to the "Share with others" list grants them the **most** privileges ("Can edit") by default. Be sure to check/adjust this every time you use the "Share" menu settings dialog.

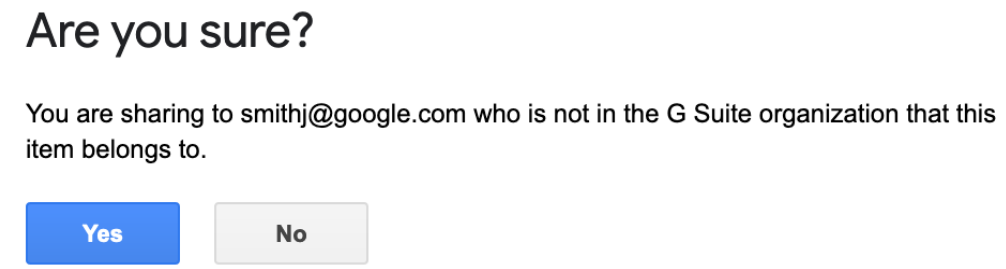


3. **Select your sharing options carefully**. Google provides a number of ways to share a file.
    a. The default is to "Share with others" by named recipient/invite. **This is the safest method** as it limits the share to specific recipients, each with an assigned permission.
        i. **It is very important to be sure you are adding the proper recipient(s)**. Pay special attention to spelling of similar names and inadvertent inclusion of student NetIDs which include a digit. (i.e. "smithj3").
        ii. **Always check the list of added recipients at least once before clicking "Send" and committing changes.**
        iii. You should only share files and folders to MSU recipients using their <NetID>@montclair.edu address. **Avoid the use of personal Google account(s) except for in very special and purposeful circumstances.** (See section 4 below for more information.)

Tip 1: External Recipient Sharing Warning

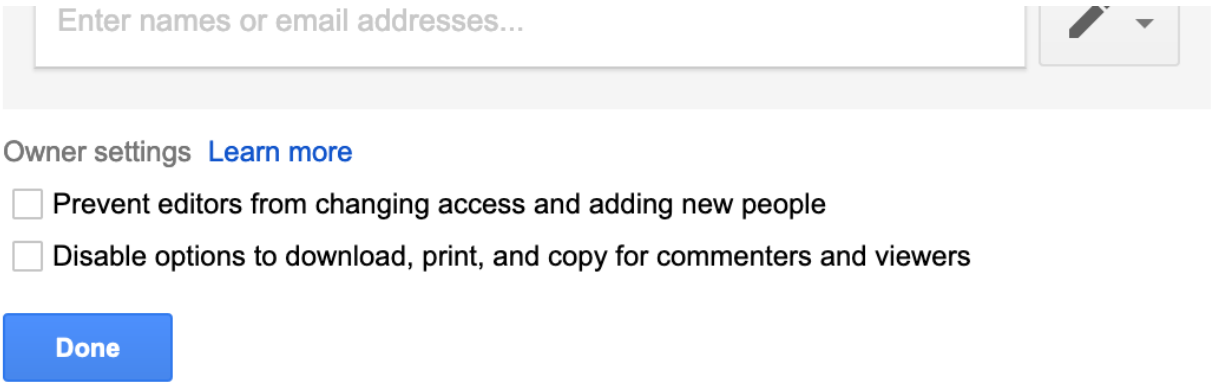
If Google detects a recipient address outside of our domain (montclair.edu), it will present a warning dialog. It is very important to be sure that external recipients are authorized to view the file/data being shared. **In general, you should think twice about sharing a file containing sensitive data to outside recipients unless absolutely necessary and approved by the data's**

owner/custodian.



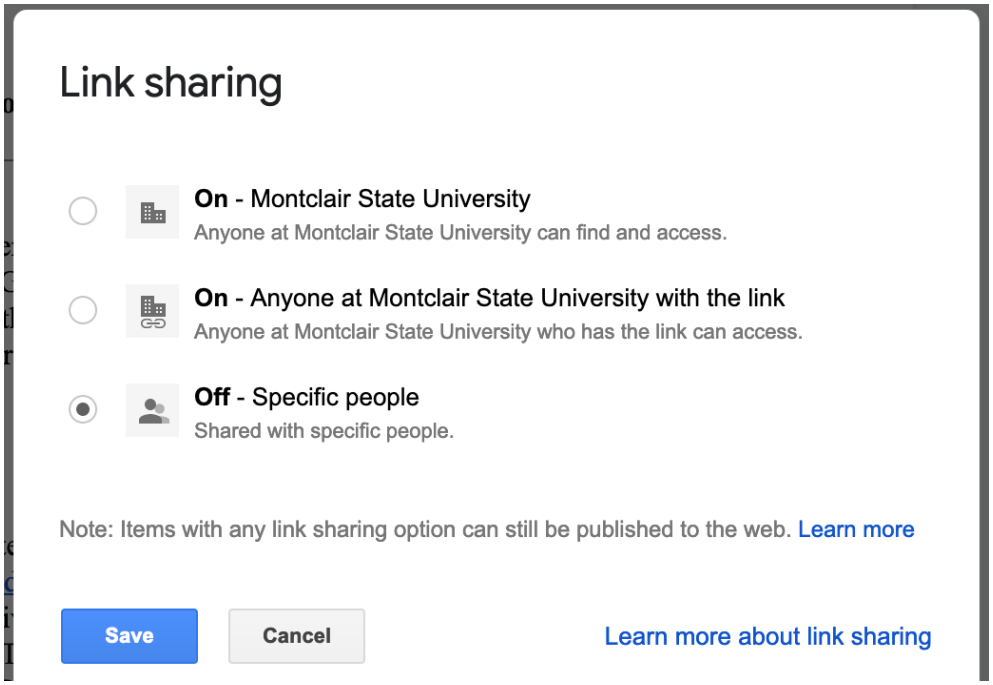
Tip 2: "Advanced" Sharing Options

On the bottom right of the "Share with others" dialog is an Advanced option. Clicking it will enable two additional options to consider in further restricting the access/abilities for recipients and should be enabled as appropriate:



---

b. Another option is to share by link ("Get Shareable Link"). **Use this option with caution as it is less restrictive** and can increase the risk of a file being accessed by an unintended/unauthorized user.



Note in particular that the second option says, "Anyone at Montclair State University who has the link can access." This means what it says-- only an MSU NetID (employee or student) is required to access the file associated with the link. So any unintentional redistribution of the link by recipient(s) will permit access to the file. **This is why link sharing introduces additional risk to access control and should only be used with files containing sensitive information in the most special of circumstances.**

Tip: Note the MSU instance of Google Drive does not permit the **public** link sharing option referenced in Google's documentation. This is an intended security measure.

---

4. **Periodically Review Sharing Settings**. Employees that separate from the University will no longer have access to their NetID and therefore Google Drive after an initial processing period and in lieu of special requests. However, in other **situations such as when an employee changes department and/or role, the file and folder share access and permissions you assigned to them will remain in place until you change or remove them**. Therefore, you should periodically review your sharing settings on all files and folders as relevant to keeping them up to date and the access control accurate. **This is also the reason to avoid sharing to an MSU user's personal Google account(s) as noted above.**

Additional Guidance and Reporting of Potential Data Sharing Concerns

As stated in the Google Drive Usage Policy and Support Agreement, support for the Google Drive service is being offered through the IT Service Desk and includes basic end-user documentation and troubleshooting assistance. When using this service, users will be expected to leverage the online help resources provided by Google wherever possible.

However, if you have a specific **security question** related to the sharing of files containing sensitive data or would like to report a concern regarding the use of Google Drive in the sharing of files containing sensitive information, please contact the Director of Information Security at: sec-official@montclair.edu.

Appendix A: Printable Reference Guide

Using Google Drive with Sensitive Data - Quick Reference

For more detail regarding the information found in this quick reference, please see the main guidance document, “Using Google Drive with Sensitive Data”.

When using Google Drive to collect, store, or share files that contain sensitive data, it is critically important that you take two key steps towards protecting the data:

1. **Protect Your Account**
    a. Practice “good credential hygiene” and ensure your NetID account password is strong, unique, and private.
    b. Enable and use Google’s 2-Step Authentication security feature.

2. **Share with Care**
    a. **Follow the principle of “need to know”**
        i. Use caution when sharing a file or folder. Only include recipients that are not only authorized but *need* to view the data in question.
        ii. Use caution when using folder level sharing. File level sharing provides more granular access control.
    b. Follow the principle of “least privilege”
        i. Do not grant a higher level of permission than recipient(s) require. Consider the actual need of each individual recipient.
    c. **Select your sharing options carefully**
        i. “Share with others” by named recipient/invite is the safest method as it limits the share to specific recipients, each with an assigned permission. Double check the recipient list before committing changes.
        ii. Use caution when enabling sharing by link as it is less restrictive and can increase the risk of a file being accessed by an unintended/unauthorized user.
        iii. Consider the advanced sharing options to further restrict the access/abilities of sharing recipients.
    d. **Periodically Review Sharing Settings**
        i. You must manually change or remove file and folder sharing settings and/or permissions for employees that change department or role.

If you have a specific **security question** related to the sharing of files containing sensitive data or would like to report a concern regarding the use of Google Drive in the sharing of files containing sensitive information, please contact the Director of Information Security at: sec-official@montclair.edu