G Suite: How to restrict access to materials

Many schools/educational bodies use G Suite or G Suite for Education to create, store and share materials. When using G Suite, it is important to make materials private. If you make materials created by other people publicly accessible, even if by accident, you may infringe copyright.

This information sheet looks at why making material private is important and provides a quick guide on how to materials private on G Suite.

Why is making materials private important?

Schools/TAFEs can use G Suite or G Suite for Education products (eg Google Docs, Google Drive and Google Classroom) to create, upload, download and share copyright materials with their staff and students. This is usually done under the relevant educational licences (Statutory Text and Artistic Works Licence or Statutory Broadcast Licence) and/or education exceptions (s28, Flexible Dealing, Disability Access Exceptions or the Exam Copying Exception).

A common requirement under these educational licences or exceptions is that access to the material is limited to staff and students. This means that if material is made publicly available, it may no longer fall under the education licences or exceptions.

Making materials private on G Suite

There are several ways you can limit who can create, access and share files on G Suite across specific organisational unit or the entire organisation. Administrators can:

- Set default access (eg restrict access to students/staff from a particular school);
- Restrict access to files in a shared drive (eg limit file access to students/staff in a particular class); and
- Control sharing of files outside your school/TAFE.

Setting up the default sharing restrictions and controlling the creation of new shared drives

This section explains how to set the default sharing restrictions to automatically control access to content in all new shared drives created by the organisation or specific organisational units. The default settings also allow you to control who can create shared drives. To set the default restrictions:

1. Sign in to your **Google Admin console** using your administrator account (does not end in @gmail.com)
2. From the Home page, go to **Apps → G Suite → Drive and Docs**.
3. Select **Sharing settings**.
4. To apply the setting to everyone, leave the top organisational unit selected. To restrict access to specific groups, **select the specific organisational unit(s)/ group(s)** (eg the specific year level or class) you want to have access.
5. Next to **Shared drive creation**, select the default restrictions for all new shared drives.
    - Prevent users in *your organisation* from creating new shared drives
    - Prevent full-access members from modifying shared drive settings
    - Prevent people outside *your organisation* from accessing files in the shared drive
    - Prevent non-members of the shared drive from accessing files in the shared drive
    - Prevent commenters and viewers from downloading, copying and printing files in the shared drive

For more information, see Control access to files in shared drives.

Restricting access to files in a shared drive and controlling who can modify the default sharing restrictions

To restrict access to files in a shared drive(s) and limit who can modify existing sharing restrictions:

1. Sign in to your **Google Admin console** using your *administrator account* (does *not* end in @gmail.com).
2. From the Admin console Home page, go to **Apps → G Suite →Drive and Docs**.
3. Select **Manage shared drives**.
4. Hover over a shared drive, and click the **Settings** button.
5. If you wish to prevent the default settings being altered, select Prevent full-access members from modifying shared drive settings to keep people from overriding the default settings for the shared drive.
6. If full-access members can modify shared drive settings, click Edit to modify any of the following options:
   - Sharing outside *your organisation*—Allow or prevent external people from accessing files in the shared drive.
   - Sharing with non-members—Allow or prevent shared drive members from giving non-members access to files in the shared drive.
   - Download, copy, and print—Allow or prevent commenters and viewers from downloading, copying, and printing files in the shared drive.

For more information, see Restrict access for an existing shared drive.

Preventing users from sharing files outside your organisation

Administrators can also limit who can move/receive files from shared drives. You can use these settings to ensure files from a shared drive are only shared within your organisation/organisational unit(s) and prevent files being moved without permission. Note changes may take 24 hours to appear and will affect all files in the drive.

You can control who can move files and folders outside your organisation in these situations:

- Moving files from a shared drive in your school/TAFE/educational body to a shared drive or My Drive owned by another organisation.
  - Only the top-level organisation can move content from the shared drive to one owned by another organisation. See Set Drive users' sharing permissions.
  - Child organisations settings only permit users to move content from a My Drive to a shared drive in a different organisation (eg another school/TAFE in your jurisdiction).
- Moving files from someone's My Drive in your organisation to a shared drive owned by another organisation

To do this:

1. Sign in to your **Google Admin console** using your *administrator account* (does *not* end in @gmail.com).
2. From the Admin console Home page, go to **Apps → G Suite → Drive and Docs**.
3. Click **Sharing settings**.
4. Select the desired **organisational unit or group**.
5. In **Distributing content outside of *your organisation***, select an **option from the table below**, then click **Save**.

Option	Description
Anyone	• Anyone with Manager access to that drive can move files from that shared drive to a Drive location in a different organisation. In addition, anyone in the selected organisational unit or group can copy content from their My Drive to a shared drive owned by a different organisation (for example, another business, group, or school).
Only users in *your organisation*	• Only people in your organisation with Manager access to a shared drive can move files from that shared drive to a drive location in a different organisation.

Option	Description
	• Users in the selected organisational unit or group can copy content from their My Drive to a shared drive owned by a different organisation.
No one	• No one can move or copy content to a drive located in a different organisation.

For more information, see Control files stored on shared drives.

For further information or advice, contact NCU at smartcopying@det.nsw.edu.au or by phone on 02 7814 3855.