OVERVIEW

What is Office 365?

Office365, also referred to as "365", is a cloud-based service which includes access to Microsoft Office applications, plus other productivity tools, over the internet.

Who Can Use 365?

The Office365 service provides popular Microsoft Office applications such as Word, Excel, PowerPoint, and OneNote in the cloud so faculty, staff, and students can work together, communicate easily, and support the University's mission.

Where is 365 Data Stored?

Data stored in Office365 services is stored at data centers owned and managed by Microsoft.

GETTING STARTED WITH 365

How do I Log In to Office 365?

To access the new Office 365, please visit **the Office 365 Portal** and log in with your OU e-mail address as the username and your OU password.

What Tools are Available?

Logo	Office 365 Tool	Purpose
	Bookings	Appointment scheduling.
E	Exchange	Email.
F	Forms	Surveys and quizzes.
	OneDrive	Storage in the cloud at no additional cost.
N	OneNote	Digital notebook.
	Power BI	Interactive visualization of data.
Power BI Desktop	Power BI Desktop	Downloadable, installed on the local workstation.
Power BI PRO 1 Year Subscription	Power BI Pro	Allows users to share live dashboards, reports, and workspaces for an additional fee.
S	SharePoint	Communication and collaboration.
S	Skype for Business	Video conferencing.
T	Teams	Integrating conversations, calls, and content.

STEP ONE - IDENTIFY DATA CATEGORY & 365 TOOL

This matrix is based on the Information Classification Standard approved by the CIO in February 2020.

Category	Type	OU OneDrive[1]	OneNote	Teams	SharePoint	Forms	Power BI
A	Healthcare Information	Add Security Settings		Add Security Settings	Add Security Settings	Add Security Settings	Add Security Settings
B	Payment Card Information	No		No	No	No	No
D1	Confidential Research & Publication Information	No		No	No	No	No
C	Student Information	Add Security Settings		Add Security Settings	Add Security Settings	Add Security Settings	Add Security Settings
D2	Research & Publications Information	Add Security Settings		Add Security Settings	Add Security Settings	Add Security Settings	Add Security Settings
E	University Administrative & Financial Information	Add Security Settings		Add Security Settings	Add Security Settings	Add Security Settings	Add Security Settings
F	Public Information	Yes		Yes	Yes	Yes	Yes

Legend: If the tool is listed as "No", it cannot be used with the coordinating category of information. If the tool and coordinating category is listed as "Add Security Settings", please review Step Three and/or OU IT Support Articles included in this guide or the OU IT Support Catalog.

[1] Only the OU version of OneDrive is approved, **not the consumer version** of OneDrive.

STEP TWO - MANAGE ACCESS

OneDrive

Because OneDrive is a cloud-based file storage and sharing utility, its use presents some potential risk to OU and its students, faculty, and staff. To properly protect sensitive information, you must understand OneDrive security and **set it up correctly**. Continue reading to learn how.

Syncing

- OneDrive allows you to automatically sync your files across multiple devices. This means that sensitive data could inadvertently end up on an insecure machine.
- If you are going to put OU data on OneDrive, we strongly recommend that you **do not sync** it to any additional locations.
- Any device you sync Category C or Category E data to must be encrypted, require a password and meet the OU's Minimum Security Standards.

File Access & Permissions

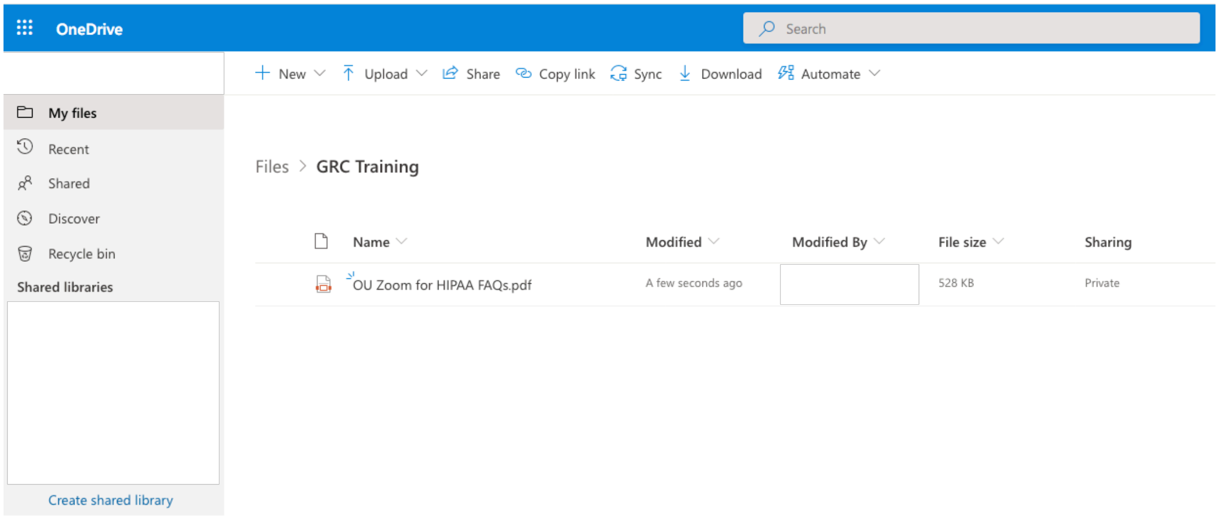
By default, only you can access the files on your OneDrive–you and anyone that can access that device. **Exercise caution when sharing files online:**

1. Sharing files with the default "Can edit" permission level allows the person you shared that file with to further share the file.
2. Pay attention! It is very easy to accidentally share the wrong folder or to share a folder rather than an individual file within a folder. Remember that the default for sharing is "Can edit", but it can be changed to "Can view".
3. Use folders to share groups of files with others online.
4. Share files with specific individuals, never with "everyone" or the "public".
5. Remember that the delivered **Shared with Everyone** folder means what it says: it is **Shared with EVERYONE**! (Office 365 makes it very easy to find documents, even if they are stored in someone else's OneDrive!)
6. Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
7. Remember that once a file is shared with someone and they download it to their device, they can share it with others.

Sharing Files Securely

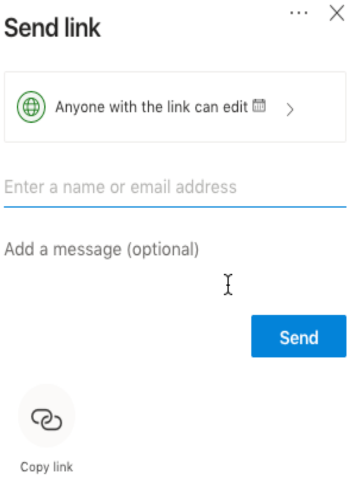
When you share files, it is important you understand how you're doing so, avoiding accidentally giving people inappropriate access to sensitive information. To do this:

1. Go to portal.office.com and sign into your Office 365 account.
2. Click OneDrive to access your cloud storage.
3. Right-click the folder or files you want to share and click Share.

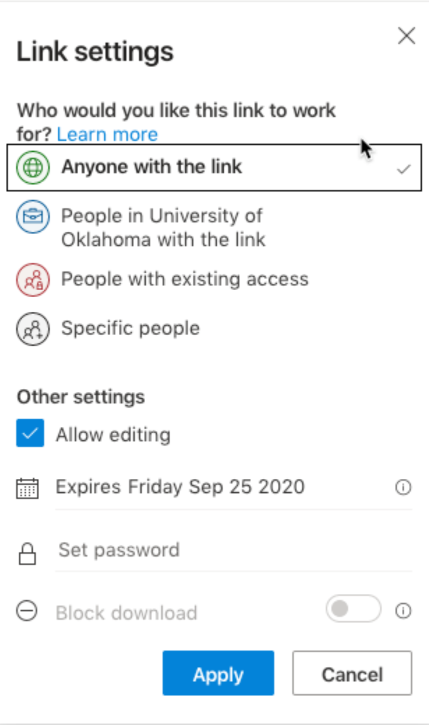


Name	Modified	Modified By	File size	Sharing
OU Zoom for HIPAA FAQs.pdf	A few seconds ago		528 KB	Private

4. Important: if you are sharing a folder you are also sharing any sub folder in that directory. Consider limiting sharing capabilities to folders that contain only information you intend to let others view.
5. Enter the names of the people you want to share with and a message, if you want.



6. (Optional) Click the drop-down list to change the type of link. The Details pane opens, where you can change who can access the link and whether people can edit the item you're sharing.



Link settings

Who would you like this link to work for? Learn more

- Anyone with the link ✓
- People in University of Oklahoma with the link
- People with existing access
- Specific people

Other settings

☑ Allow editing

Expires Friday Sep 25 2020

Set password

Block download

Options for Sharing

- Anyone gives access to anyone who receives this link, whether they receive it directly from you or forwarded from someone else. This may include people outside of your organization.
- People in University of Oklahoma gives everyone with an OU login name access to the link, whether they receive it directly from you or forwarded from someone else.
- Specific people give access only to the people you specify, although other people may already have access. If people forward the sharing invitation, only people who already have access to the item will be able to use the link. **We strongly encourage you to always use this option.**
- By default, allow editing is turned on. If you want people to only view your files, uncheck the check box.
- The expiration date allows you to define temporary access to the document, with access expiring on the date set in this field.
- Set password, allows you to further restrict access to the document to those with the link and the password.
- Block download allows you to prevent collaborators from downloading the document. We strongly encourage you to use this option when sharing Category A, Category C, and Category E data.

7. When you’re done, click Apply.
8. When you’re ready to send the link, click Send.
9. Review sharing privileges in OneDrive on at least a quarterly basis:
   - Access MS Teams using any version of the app.
   - Click open in OneDrive to access your Teams cloud storage.
   - Click Settings (the gear icon in the upper right-hand corner).
   - Click OneDrive Settings, and click More Settings.
   - Click Run sharing report. You will be prompted to select an existing or create a new OneDrive folder to store this report. Select the desired location and click Save. OneDrive will send you an email confirmation when the report is ready for viewing.
   - Remove individuals that no longer require access to files or folders.

Teams

By default, only Teams members can access stored files.
Exercise caution when authorizing access to Teams files.

1. Create different channels in Teams to direct conversations to authorized individuals only.
2. Share files to Teams with specific individuals, never with "everyone" or the "public".
3. Regularly review shared files by clicking the Files menu in any version of the Teams app (mobile, desktop, or web), and selecting Microsoft Teams or Recent to view history.

SharePoint

By default, only SharePoint members can access stored files.
Exercise caution when authorizing access to SharePoint sites.

As required by regulations and recommended by industry best-practices, SharePoint allows Site Owners to grant access to data upon a user’s request in emergencies like imminent danger to the health and safety of a person or the public. Also, SharePoint offers to assign access rights to individual files. Protect OU data stored in SharePoint by:

1. **Use groups to manage permissions**. Many Site Owners, if they want to quickly grant access to SharePoint, assign permissions directly to users. Assigning permissions to users can potentially expose OU data to those who are not authorized, causing leaks of sensitive information and creating more work for the Site Owner. SharePoint security is permission driven. There are three main security groups in SharePoint:
   - Site Visitors are read-only users who can view and download content from SharePoint sites.
   - Site Members can read, download, add, edit, delete and share content.
   - Site Owners are full-control users who do everything Visitors and Members can plus they can configure site security, add web parts, etc.
2. **Decide site members and access levels**. Carefully think through which users need access, and to what level.
3. **Leave Item-Level permissions as they are**. Item-level permissions can be used as a quick fix to grant access to specific files, but you should avoid using them wherever possible. SharePoint does not offer an easy way to see and administer all of the special permissions assigned in this way, and it is easy to lose track of access. Instead, group items into libraries or folders and assign permissions to the groups of files.
4. **Break inheritance**. To restrict access to those who need-to-know, Site Owners can block permission inheritance at any level in the SharePoint hierarchy.
5. **Page permissions.** Edit page permissions to limit users with the Contribute permission level the ability to click on the Page Tab, Edit button and start moving around (or deleting) elements on your pages.
6. **Review access**. Regularly review SharePoint access lists on a quarterly basis.

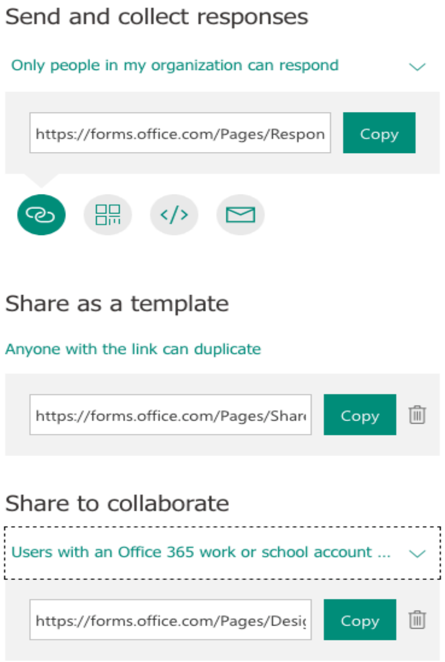
Forms

You can control whether or not external users are allowed to collaborate with users in your organization on a form or quiz.

On the **Microsoft Forms** pane, the **Share** setting has three options:

1. Send a link to the form to people outside of your organization and collect responses from external people.
2. Collaborate on the form (e.g. edit questions, change the theme design) with people outside of your organization.

3. Share the form as a template so people outside of your organization can duplicate the form for their own purposes.



Send and collect responses

Only people in my organization can respond

https://forms.office.com/Pages/Respon

Share as a template

Anyone with the link can duplicate

https://forms.office.com/Pages/Share

Share to collaborate

Users with an Office 365 work or school account ...

https://forms.office.com/Pages/Desig

STEP 3 - ADDITIONAL SECURITY SETTINGS

OneDrive File Syncing

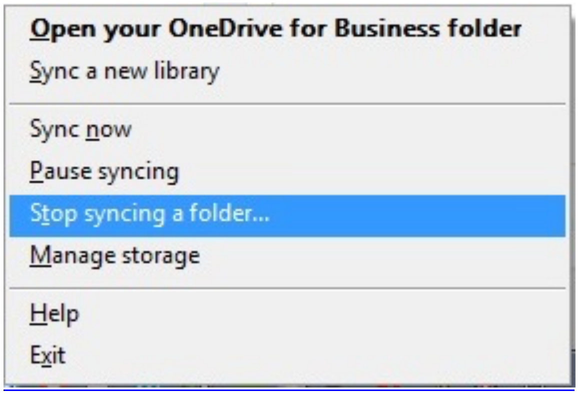
If you decide to sync OneDrive across multiple devices, be sure the security on the devices that your information is synced with meets the minimum-security standards below:

- Install virus/malware detection software with the latest definitions.
- Run a firewall that blocks in-bound traffic.
- Do not log into your workstation or device as an administrator (unless absolutely necessary).
- Keep your operating system and software up to date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- Talk to your departmental IT support for help securing your computers and other devices.

Syncing across multiple devices inherently creates the potential for unintended data leakage; syncing *Category A* data is therefore strongly discouraged. Always take caution when transmitting sensitive information.

By default, OneDrive is set up to sync all files and folders, but you have the ability to customize what is synced.

1. Open your OneDrive app settings and navigate to Sync Settings.



2. Choose which folder(s) you decide to sync. Stop syncing any folders you choose.

SharePoint Sharing Levels

In SharePoint, sharing is implemented at two levels:

1. Organization Level
   - For any external sharing to be allowed, it has to be enabled by OU.
2. Site Level
   - Once enabled across the organization, external sharing can be restricted on a site-by-site basis. Global or SharePoint admins in Office 365 can change the external sharing setting for a site, but site owners cannot do this.

In some cases, there might be a mismatch between these two levels. In that case, the more restrictive of the two policies is the one applied.

Types of External Users

In SharePoint, if you share with a user who is not in the OU directory, they are sent a one-time code that they can use to verify their identity. The next aspect of sharing to understand is that SharePoint supports four basic options when it comes to external sharing and that each option allows your files to be accessed by different types of user:

No External Sharing:

The default option for communication and classic SharePoint sites. If this option is enabled, it will prevent any site users from sharing any site content externally. This can be a good option for sites that only your team need to have access to. To use this option, go to your SharePoint admin center, and in the left pane under Sites select Active sites. Select the proper site, and then click Sharing. Select the Only people in your organization option and select Save.

Authenticated: Existing Guests

Existing Guests allows external sharing with users who already appear in your Azure Active Directory. External users will appear here if they have previously accepted sharing invitations, or if you manually added them in the Azure Portal. To use this option, go to your SharePoint admin center, and in the left pane under Sites select Active sites. Select the proper site, and then click Sharing. Select the Existing guests' option and select Save.

Authenticated: New and Existing Guests

New and Existing Guests allows new users to access your files via an invitation link. To use this option, go to your SharePoint admin center, and in the left pane under Sites select Active sites. Select the proper site, and then click Sharing. Select the New and existing guests' option and select Save. As an administrator, you can share a site with new users, and site users can share any files held on this site. When they share a file, the new user will receive an email invitation with a link. They will then either sign into their Microsoft account or enter a verification code. If they use a Microsoft account, they will be automatically added to your Azure Directory. If they use a verification code, they won't be, and they will have to use a code every time they want to access files.

Anonymous Sharing:

If you use this option, anyone with a link will be able to view and edit the relevant files. This can be a quick way of giving external users access to your files, but you should be very careful when using it, because you will have little oversight as to how your files are being accessed, used, and further shared. To enable this option, go to your SharePoint admin center, and in the left pane under Sites select Active sites. Select the proper site, and then click Sharing. Select the Anyone option and select Save.