



Permissions and Sharing in SharePoint Online

What does this guide cover?	Maintaining permissions, access control and sharing in SharePoint Online sites
Who is it aimed at?	SharePoint Network Administrators (SNAs) and Site Owners

Introduction

This document covers the various permissions settings and application of sharing for external (non-University) and internal (University) SharePoint Online Users.

Permissions Overview – What are the defaults?

The same but different?

SharePoint Online permissions can be as simple or as complicated as your site use requirements. Essentially, SharePoint Online has the settings you may have used in SharePoint on-premise, but with some new features and service-wide integration that can offer more potential for access control and sharing.

[Learn more at Microsoft's SharePoint Online Permissions Page](#)

Depending on the type of site you have requested, you will have the following permissions options by default:

In a Team and Communications Site:

Team and Communications Sites			
Overseen by Site Network Administrator			
Group	Site Owners	Site Members	Site Visitors
Permissions	Full Control	Edit	Read
Actions	<ul style="list-style-type: none"> • Create new libraries • Create lists • Change permissions • Alter navigation • Change page layouts 	<ul style="list-style-type: none"> • Edit existing content 	<ul style="list-style-type: none"> • View existing content • Navigate through site

Overview of permission groups for Teams and Communications sites

Site Administrators: although this is NOT strictly a permission group or level, multiple site administrators can be assigned in a role akin to the previous Site Collection Administrator role in SharePoint on-premise

- **<SiteName> Owners** – Members of this group “own” the site and have the second highest level of access, can create new libraries, lists and other apps within the site, change permissions for users, alter navigation and page layouts etc. Sharing is also enabled for Owners only by default
- **<SiteName> Members** – Members of this group can edit existing content in the site but cannot typically change navigation, assign permissions etc
- **<SiteName> Visitors** – Members of this group can view items, navigate through the site but cannot edit items nor alter permissions

If you have requested that your site allows sharing with external users, you can share items and assign the above permissions to existing, known external users, referred to as “firstname lastname (Guest)”, such as those who have been previously assigned membership of a Microsoft Team.

External Users – No more temporary accounts or virtual cards!

Streamlined external collaboration across all Nexus365 services including SharePoint Online.

For the first time, external access to SharePoint Online won’t require either a temporary separate external user account or a virtual card for access to the service. In line with OneDrive for Business and Microsoft Teams, External users can read or collaborate on content in a SharePoint Online site using either their own Microsoft accounts (other provider accounts will also work but may see reduced functionality, particularly when trying to edit documents in place, which works best with a Microsoft account).

[Find out more about what happens when users share on Microsoft’s External Sharing Page](#)

NOTE! By default, all sites regardless of site type will be created with external sharing disabled. The provisioning form will ask you specifically if you want to switch it on.

One other security measure to note is that only Site Owners will have the ability to share items externally. We also recommend that you do NOT grant site ownership to external users for this reason, in order to offset the risk of a data breach, instead making them Site Visitors (the default) or Site Members. In operation, this will be entirely at the discretion of the site administrators / Site Owners / SNAs.

Custom Permissions and Groups

When you want more granularity

As with SharePoint on-premise, SharePoint Online allows you to create additional SharePoint groups in your site and additional custom permission levels to assign to those groups.

[Find out more on Microsoft’s page on custom permissions and groups](#)

Available to Site Administrators and Site Owners, this allows you to create SharePoint groups with fine-tuned permission levels to suit your access control needs. For example, allowing or disabling downloading of files from a document library, or allowing users to set up their own custom views of a list. This behaves in an identical way to SharePoint on-premise so should be familiar to the majority of users.

Unit-Level (pre-populated) Groups and Office365 Groups

Starting with a whole collection of users in either of the above types of group

Both Unit-Level (CUD Affiliated) groups and existing Office365 Groups (such as the groups that get created alongside your Microsoft Teams or standalone groups created via OSM Request) can be added to SharePoint Groups in order to pick up the permissions assigned to them automatically. The Unit-level groups work in much the same way as they did in SharePoint on-prem so when you start typing the name of your unit into a people picker when adding members to an SharePoint Online group, you may see something like this:

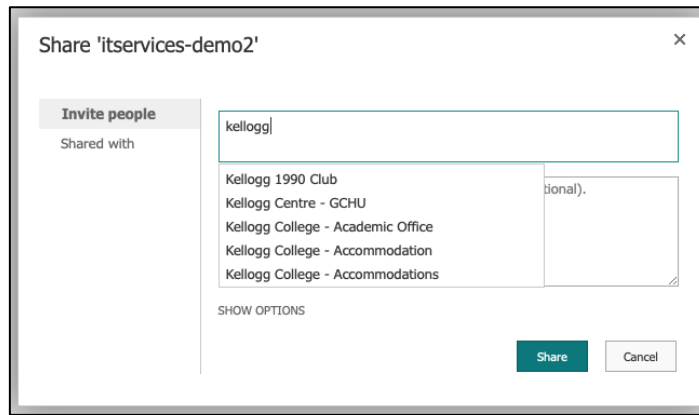


Figure 1. Screenshot of SharePoint Online, showing interface for adding members to a site

Members of these groups are added by unit affiliation, usually by a Unit’s HR department. Memberships of these groups are not visible through SharePoint Online, but they are usable if you want to grant broad access to a large collection of users in your unit based on their status, such as staff, cardholders or students.

Note! Mailing Lists such as Sympa or external mailing lists are not supported in SharePoint Online, Teams or OneDrive for Business. Do add mailing list email addresses to your shares or sites as you will literally just be adding the first person in the mailing list to respond to the sharing or access email!

Office365 Groups can also be added to a people picker in the same way. If you know the name of the group, or its email address, you can type that into your people picker window in your SharePoint Online group to have all the members of that group granted access.

One final note – clicking the “Show Options” link in the group add / people picker window as shown above exposes one very important control:

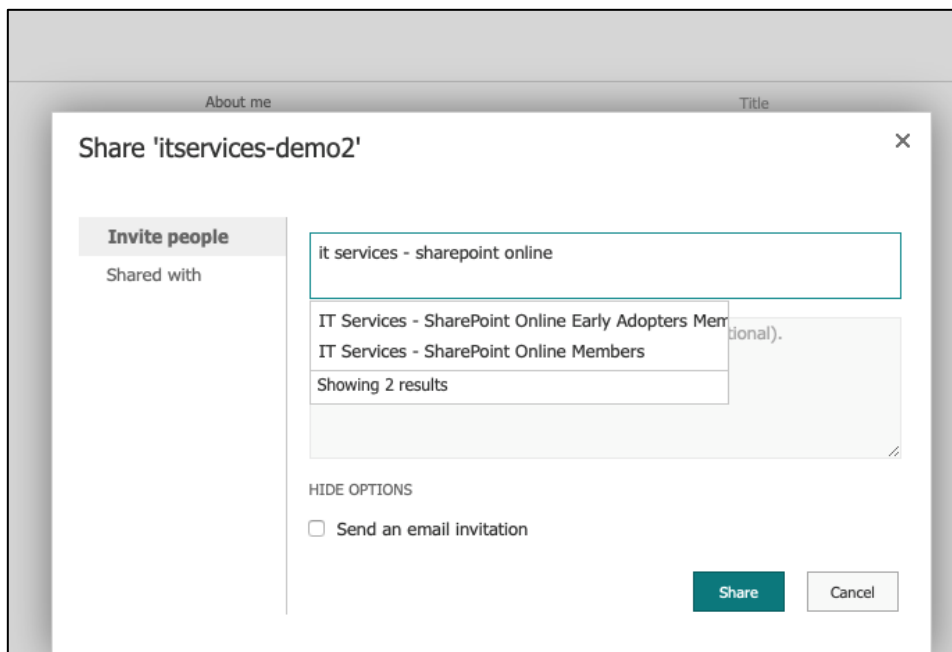


Figure 2. Screenshot of SharePoint Online, showing interface for adding members to a site, including the “send an email invitation” option underneath

By default, the “Send an Email Invitation” box under ‘show options’ is ticked, meaning that if you add a large group to a SharePoint Online group, all members of the group will get an email telling them you just shared your SharePoint Online site with them. This is not advisable for large unit-level or O365 groups!

You can also type ‘everyone’ into your people picker, to be presented with this option:

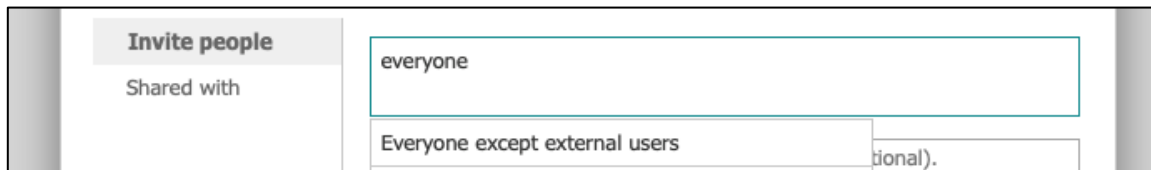


Figure 3. Screenshot of SharePoint Online interface for adding members to a site, showing how to add everyone in the organisation

This does exactly what it says; it allows everyone in the entire organisation to view (or edit) your site if added to a SharePoint Group. This may be useful if you’ve set up a site where you’d like everyone in the University to be able to access your content, but again, remember to untick the blue tick box under ‘more options’ unless you want to potentially email everyone – which is **not** advisable!

Best Practice Tips and Notes

Making managing permissions less of a headache

Setting up and controlling permissions in your SharePoint Online site is important to get right, else it can turn into the largest source of support calls to the Nexus Team regarding SharePoint.

We recommend that you consider the following points when starting out with SharePoint Online permissions to ensure that you get the best use out of the service and avoid the potential pitfalls of over-complicated permissions schemas in your sites.

- Consider the requirements of your site before provisioning. How many users will it have? How many different permission levels will you need? Will the three default SharePoint Groups be sufficient? Can you better manage a site and its content through Office365 Groups?
- Always consider the “more sites are better” model for SharePoint Online. Rather than creating one huge site collection containing multiple subsites, libraries, folders and individually controlled items, always consider setting up new sites for specific sets of users or specific use cases
- For collaboration purposes, consider using Teams as the place to work on documents or content, using SharePoint Online as your publishing portal for information you wish to share further or with more granularity
- Consider that for every item you break permissions inheritance on, whether a library, list, folder or individual document, you set up a new permissions management item that you will have to manage
- Also consider that for every item you hit the ‘share’ button on, you will do the same – setting up an individual permission level for something that would be far better managed as part of a site, a Microsoft Team or a library / list with group-based permissions
- Unlike Microsoft Teams, External users of your site can be joined to either the Site Owners SharePoint Group, or can be named as site administrators. For security reasons we would strongly advise against these actions and would urge you to consider how powerful both roles are in respect to what each role is capable of within the permissions schema of a site

Information Security

When using manually-maintained permissions:

1. You must remove permissions promptly once they are no longer needed, such as when people leave or move roles, including permissions given to external users. You may want to ensure there are processes in place for people to notify you when this happens
2. You should not rely on SSO account expiry, even for internal users
3. You must periodically review all permissions on your site