

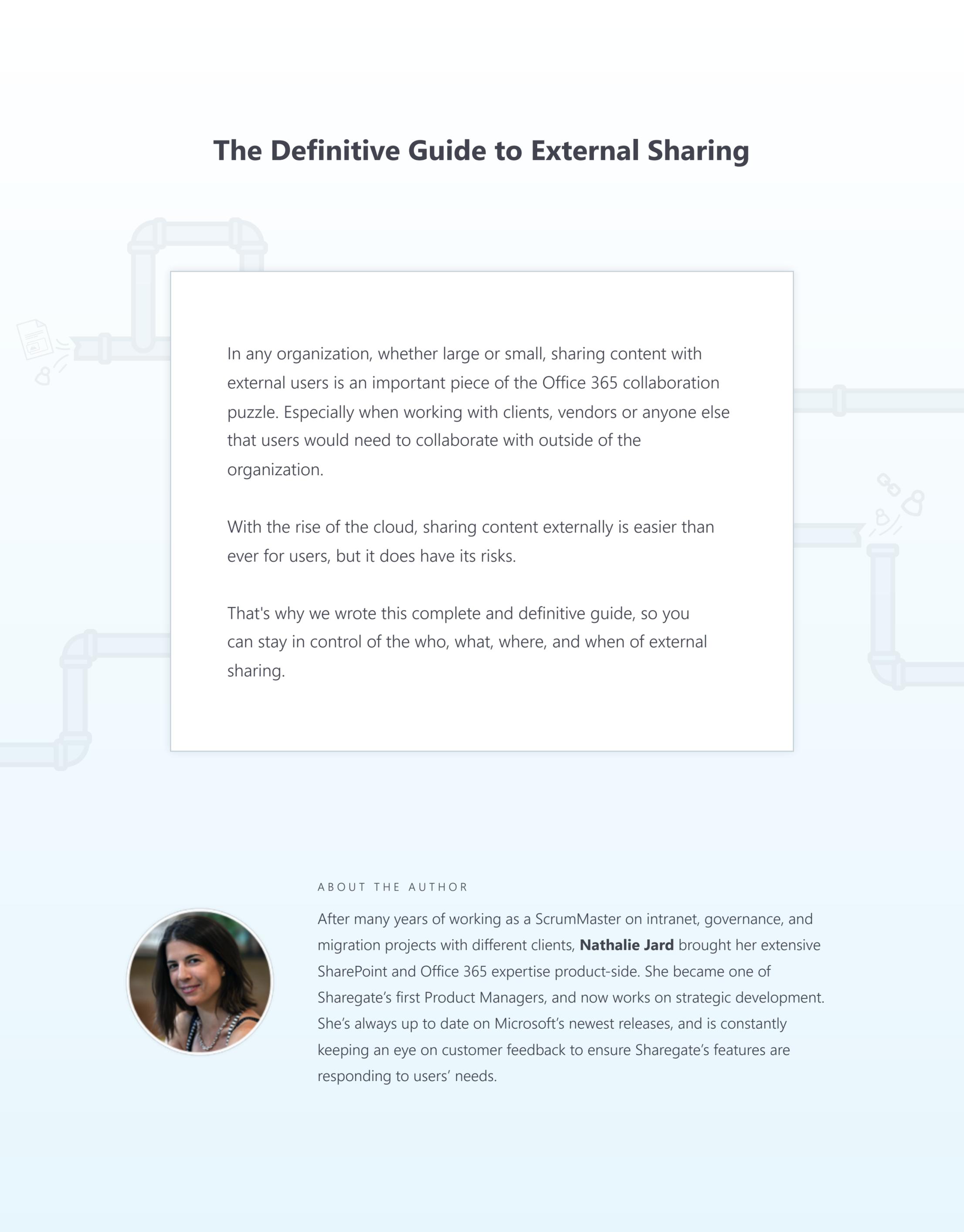
The Definitive Guide to Office 365 External Sharing

An eBook by **Sharegate**



Osio

The Definitive Guide to External Sharing



In any organization, whether large or small, sharing content with external users is an important piece of the Office 365 collaboration puzzle. Especially when working with clients, vendors or anyone else that users would need to collaborate with outside of the organization.

With the rise of the cloud, sharing content externally is easier than ever for users, but it does have its risks.

That's why we wrote this complete and definitive guide, so you can stay in control of the who, what, where, and when of external sharing.

ABOUT THE AUTHOR



After many years of working as a ScrumMaster on intranet, governance, and migration projects with different clients, **Nathalie Jard** brought her extensive SharePoint and Office 365 expertise product-side. She became one of Sharegate's first Product Managers, and now works on strategic development. She's always up to date on Microsoft's newest releases, and is constantly keeping an eye on customer feedback to ensure Sharegate's features are responding to users' needs.

CHAPTER ONE

What Is External Sharing?



On the surface, external sharing in Office 365 is the act of making content available to someone outside of your organization.

Behind the scenes though, it can mean very different things depending on whether or not the content is shared **anonymously** or with an **authenticated external user**.

1. Sharing with Anonymous Users

A folder or document can be shared with an external user via an anonymous link, meaning the person accessing the document can't be identified by the organization. These guest users are commonly called "anonymous users".

When this option is chosen, your document will be visible to anyone who has access to the link, meaning an external user to whom it was sent to directly can share the link to other external users. Thus, documents containing sensitive data should never be shared this way.

The person choosing to send a document anonymously can decide whether to make it "View Only" or "Editable". They can also set an expiration date, so the content isn't accessible to external users after the chosen date.

In essence, the permissions to access your content is **given to the hyperlink** and not a user.

2. Sharing With Authenticated External Users

Content can also be shared with authenticated external users, meaning guest users are sent an invitation by email and prompted to sign in using an account from a trusted provider in order to access the content in question.

Once the invitation is accepted, they are added to your organization's directory as an external user, but will only have access to the specific elements you shared with them. If you've shared an entire site, they'll have access to everything in it, so make sure it doesn't contain sensitive content.

If you want to see whether or not the user has accepted the invitation and accessed your content, you can view pending invitations in your site collection settings, under the

tab "Access requests and invitations," or you can search the guest user's name in your directory.

	External Authenticated Users or Guest Users	Anonymous Guests
Particularity	<ul style="list-style-type: none"> • Signing in is required before they can view content 	<ul style="list-style-type: none"> • Can access content from a shared link without signing in
What you can share	<ul style="list-style-type: none"> • A complete site • Lists and Libraries • Documents and list items • Yammer threads • Teams (coming summer 2017) • Some content within an Office 365 Group 	<ul style="list-style-type: none"> • Only documents or folders
Who can share	<ul style="list-style-type: none"> • Site owners and others with full control permissions can share a site • All members as contributors can share lists, libraries and documents • All members can nominate a person to be added in an Office 365 Group as a guest user 	<ul style="list-style-type: none"> • All site users can share a document and generate a view or edit link for external sharing
What kind of sharing	<ul style="list-style-type: none"> • The same as with your internal users 	<ul style="list-style-type: none"> • View only link • Edit link
What are the security risks	<ul style="list-style-type: none"> • If you give full control to an external user, he could share content with other external users • It's hard to link the email address you sent the invite to and the Microsoft account associated to the user • Permission inheritance if you give access to a site or a Group 	<ul style="list-style-type: none"> • Anonymous guest links can be shared to other people who might be able to view or edit the content. • Changes cannot be tracked in the document.

CHAPTER TWO

How to Configure External Sharing?



Because of the risks associated with external sharing, most Office 365 administrators prefer disabling it entirely.

This can lead to a multitude of other problems, like employees using other third-party tools such as Box.com or Google Drive, to send documents. This could result in administrators losing control over what is shared externally.

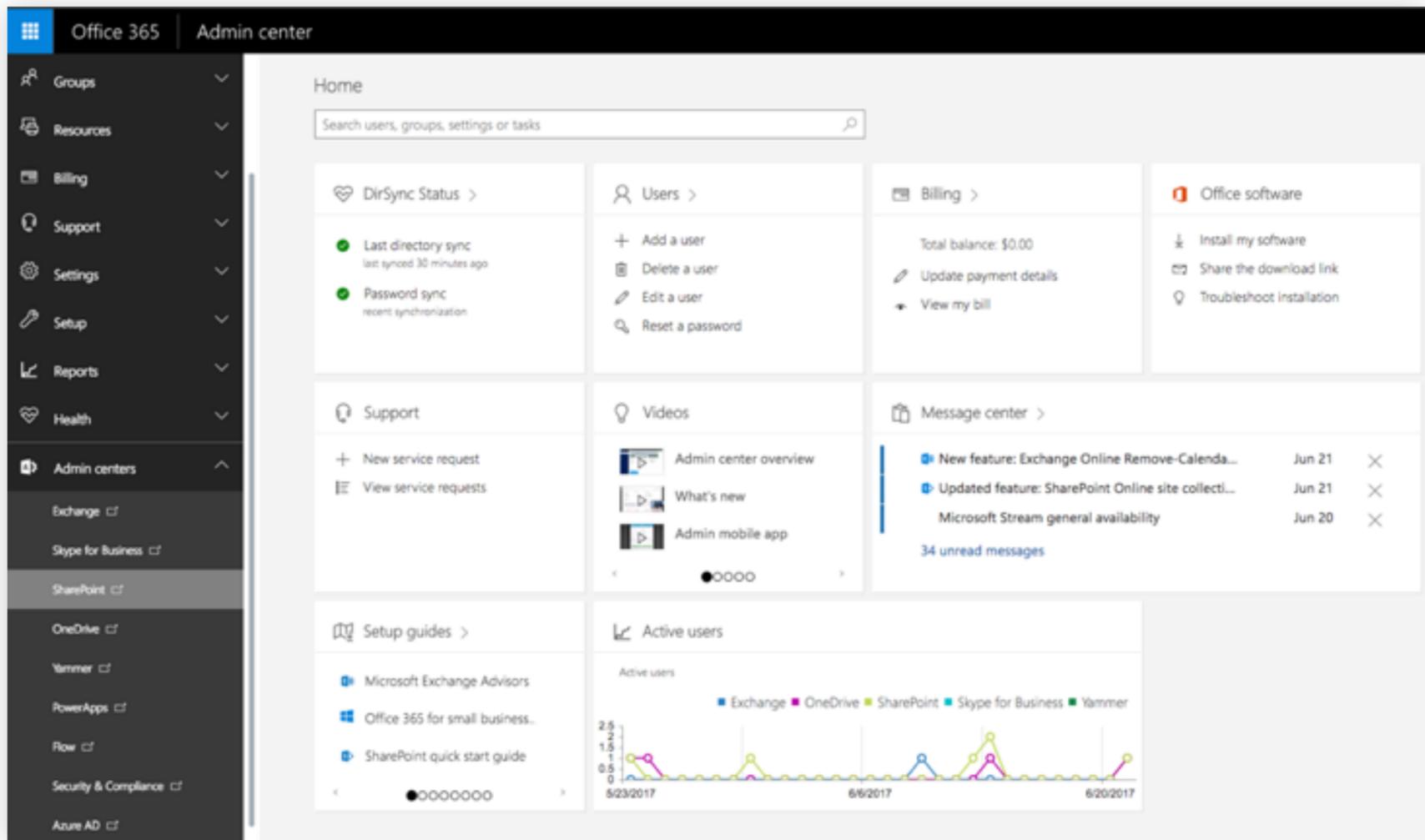
That's why it's important, as the administrator of your tenant, to configure external sharing settings to the needs of your organization, rather than simply turning it off. Employees will find a way to accomplish their daily tasks, so you might as well provide them with what they need from the beginning!

This is how you configure external sharing in SharePoint, OneDrive for Business and in Office 365 Groups.

External Sharing Configuration in SharePoint

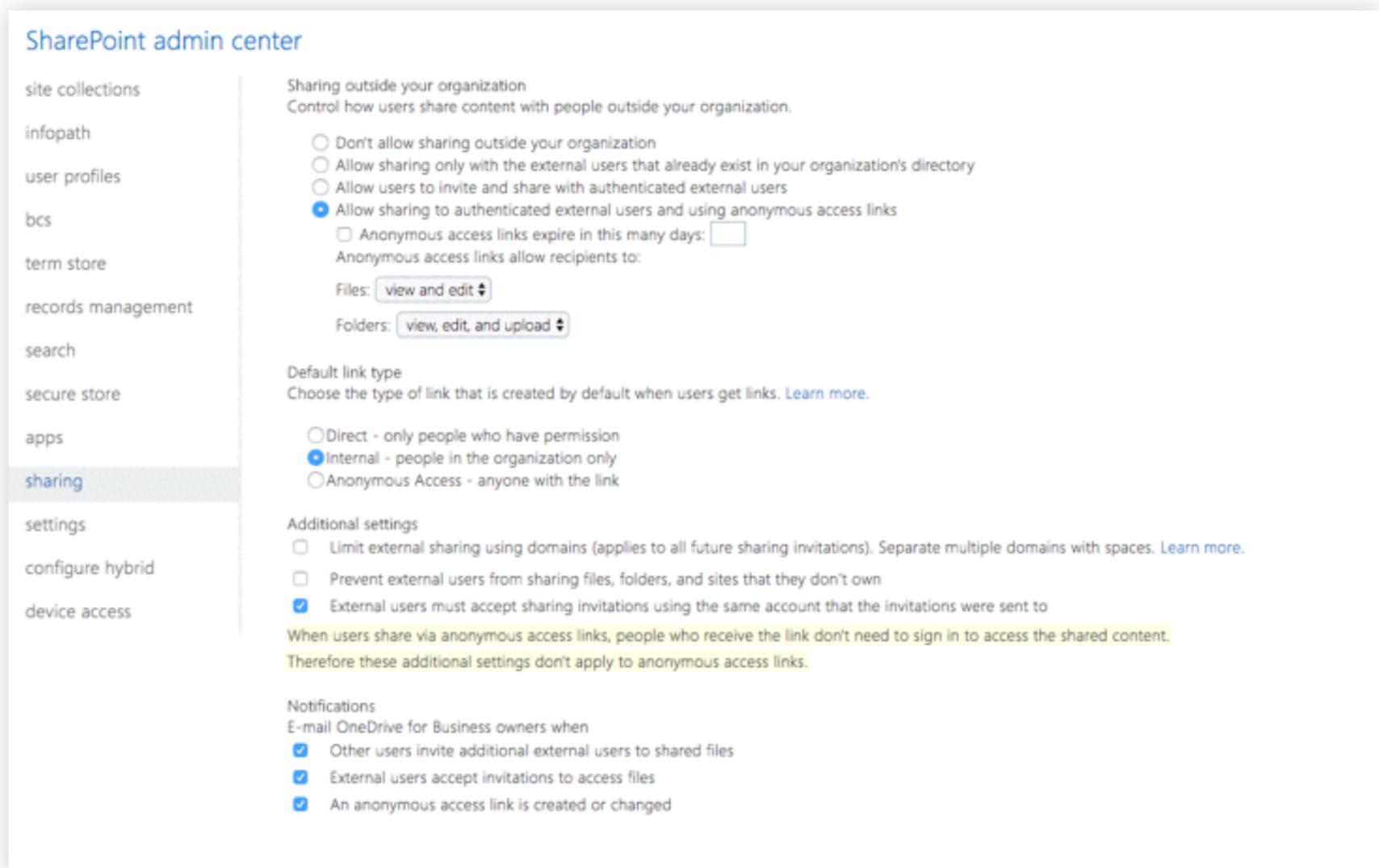
Before managing External Sharing for SharePoint, you'll have to make sure it's enabled for your Office 365 tenant as a whole. This can be found under the Security & Privacy tab of your Settings menu within your Tenant Admin Console. There, you can control external sharing globally first.

1. From your Office 365 home screen, navigate to your Admin center.
2. From the Admin center, choose the "Admin centers" tab on the left-hand side and then "SharePoint ." This will take you to the SharePoint admin settings page, where you can configure external sharing.



3. Navigate to the "Sharing " tab on the left to view all of the sharing options. In this case, we'll only talk about the top section. The rest we'll discuss in the next chapter, on managing external sharing.

It's important to note that, by default, external sharing is allowed, anonymously or not, in your organization. This setting should be adjusted to your specific business needs to avoid accidental data leaks.



Here are the available options that you can choose from when configuring external sharing:

"Don't allow sharing outside of your organization."

As the name suggests, this option blocks access to your tenant for anyone outside of your organization.

"Allow sharing only with the external users that already exist in your organization's directory."

When an External User is added to your organization, it's in fact creating an Active Directory object in your Azure Active Directory. In other words, the user is created, but it's a special type: a guest user.

This option tells your SharePoint environment that only these users, created at a previous time, can be granted access to content in your tenant. An admin can manually create these external users in their Azure Active Directory via the Azure Portal, but SharePoint will not facilitate the creation of new users through its' sharing interface.

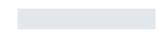
"Allow users to invite and share with authenticated external users."

Enabling sharing with authenticated external users means allowing your employees to invite new guest users to your directory and share specific content with them, without an administrator's direct approval.

They will be visible in your directory as guest users, so these permissions can be cleaned up if you see documents have been shared with people they shouldn't have.

"Allow users to invite and share with authenticated external users and using anonymous access links."

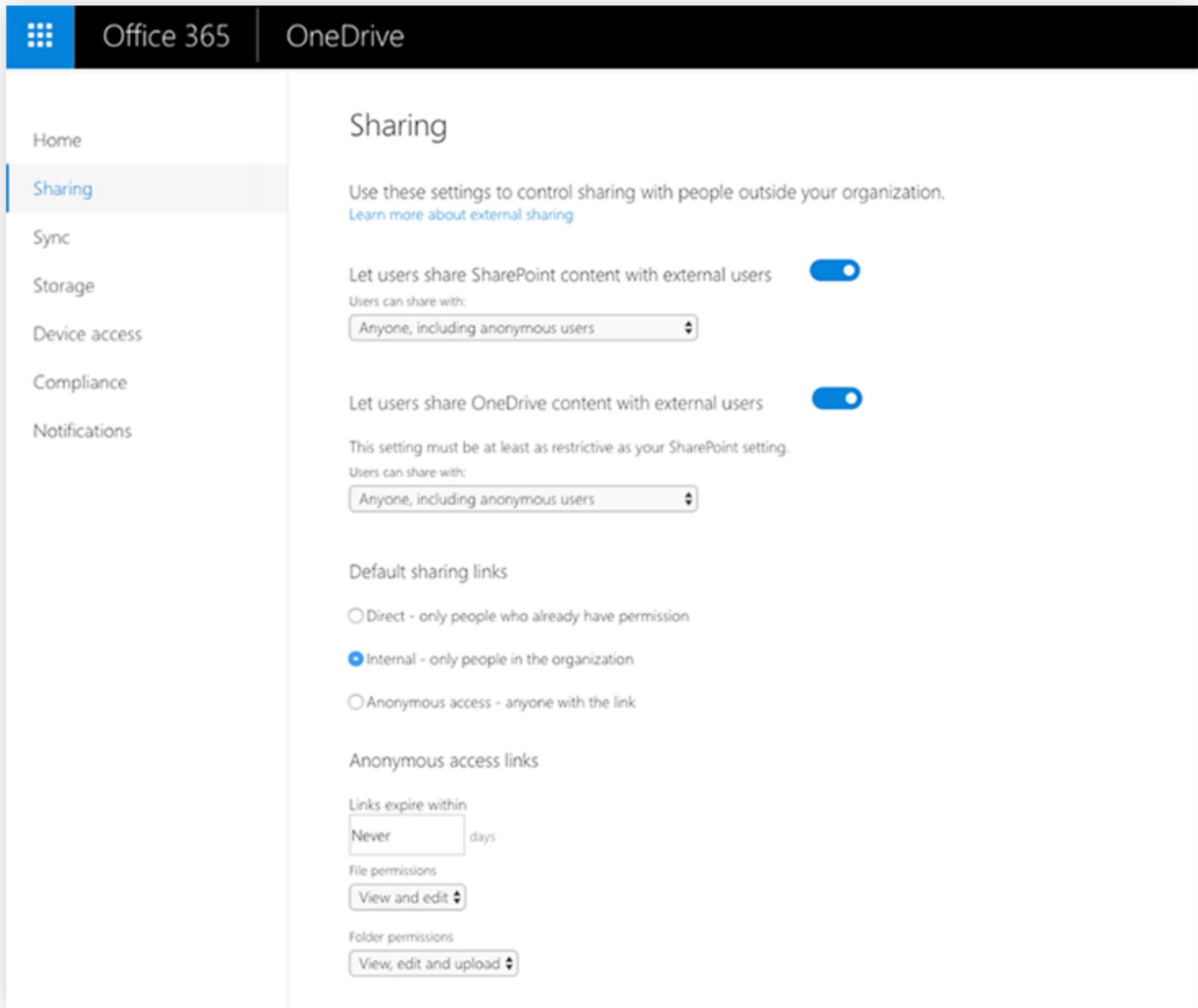
This level of external sharing sums up what we've already described in the previous chapter. Authenticated external users can be invited to log in and view or edit documents, but anonymous users can also be shared with if the owner of the document chooses to share an anonymous link.



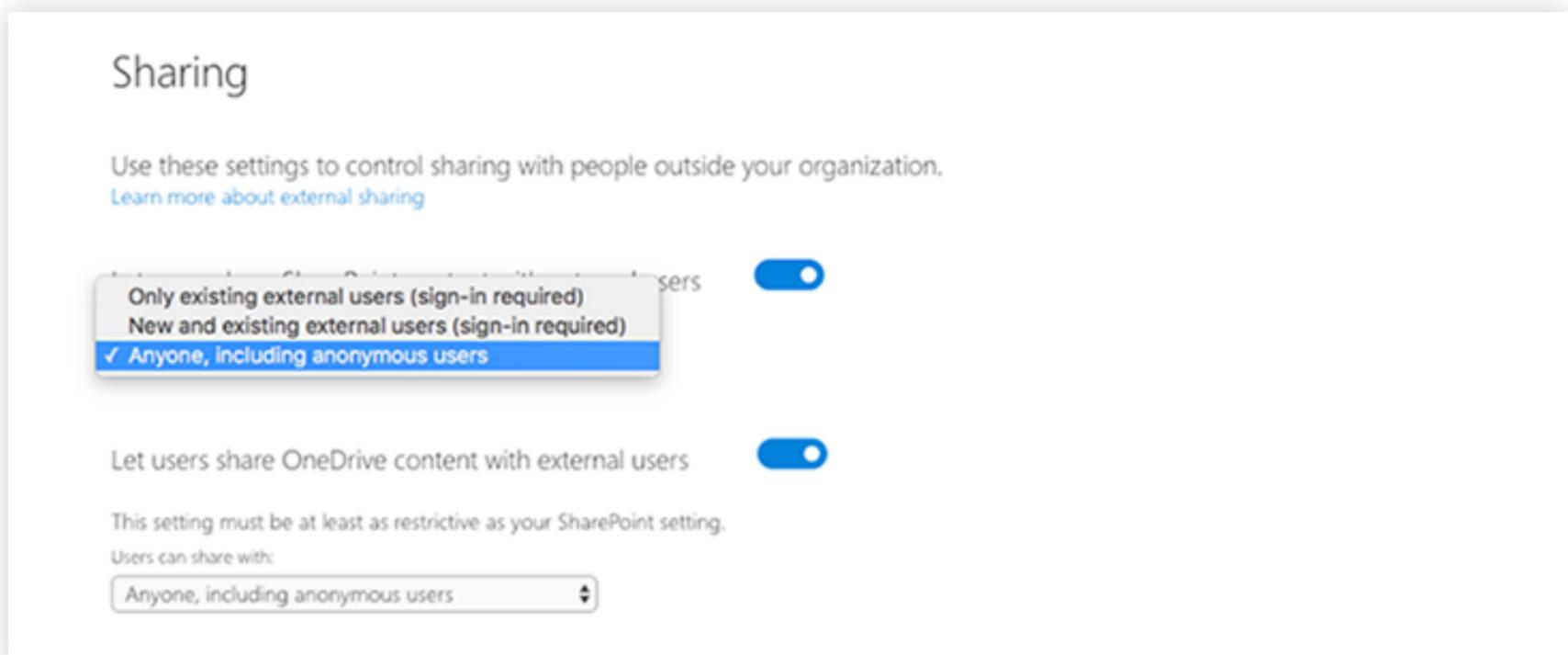
External Sharing Configuration in OneDrive for Business

By configuring external sharing here in the OneDrive admin center, it also controls the external sharing options in your SharePoint Online.

1. The first three steps are identical to that of getting to the SharePoint admin center, but obviously by choosing the "OneDrive" tab.



2. The options in the OneDrive external sharing settings are the same as SharePoint, but the UI is a little different. The same options are available, but in a drop-down menu rather than by radio buttons.



CHAPTER THREE

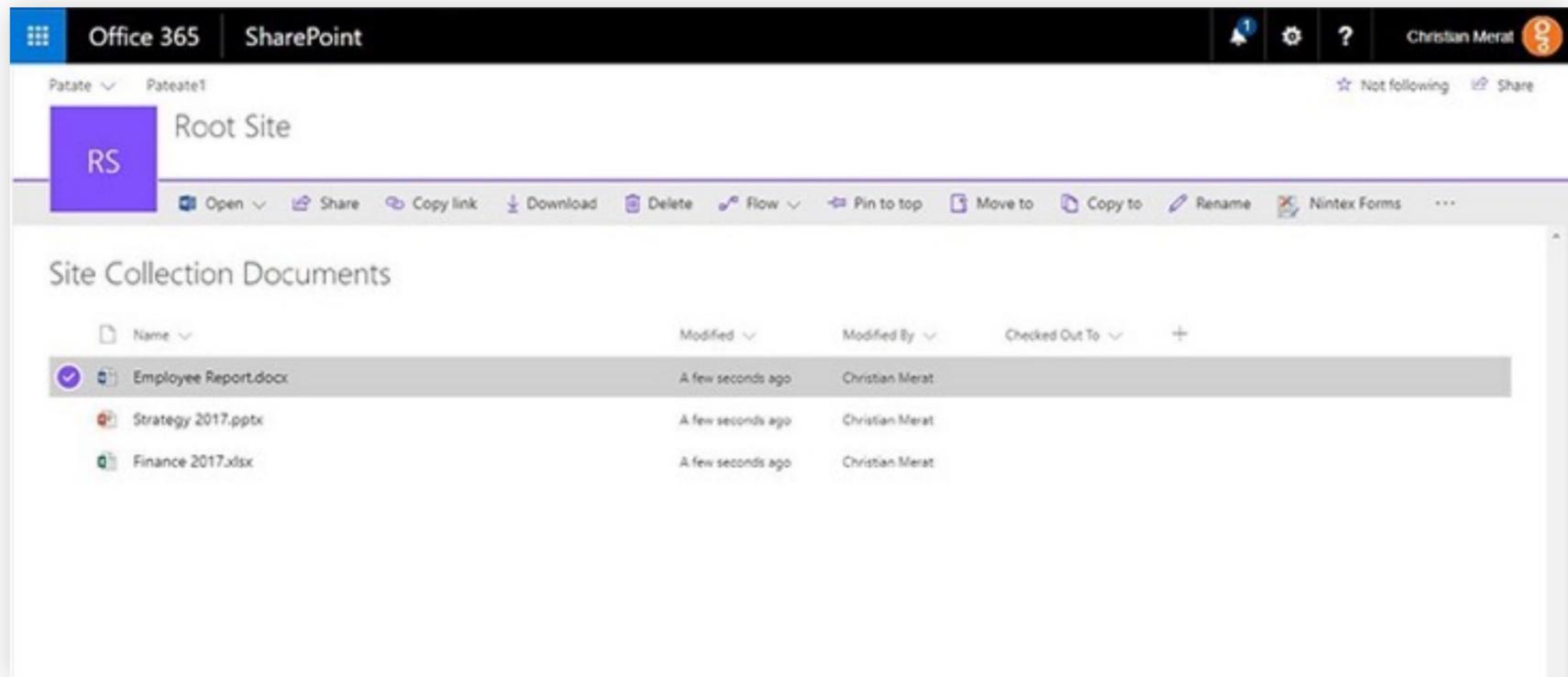
How Can Users Share Externally and What Happens When They Do?



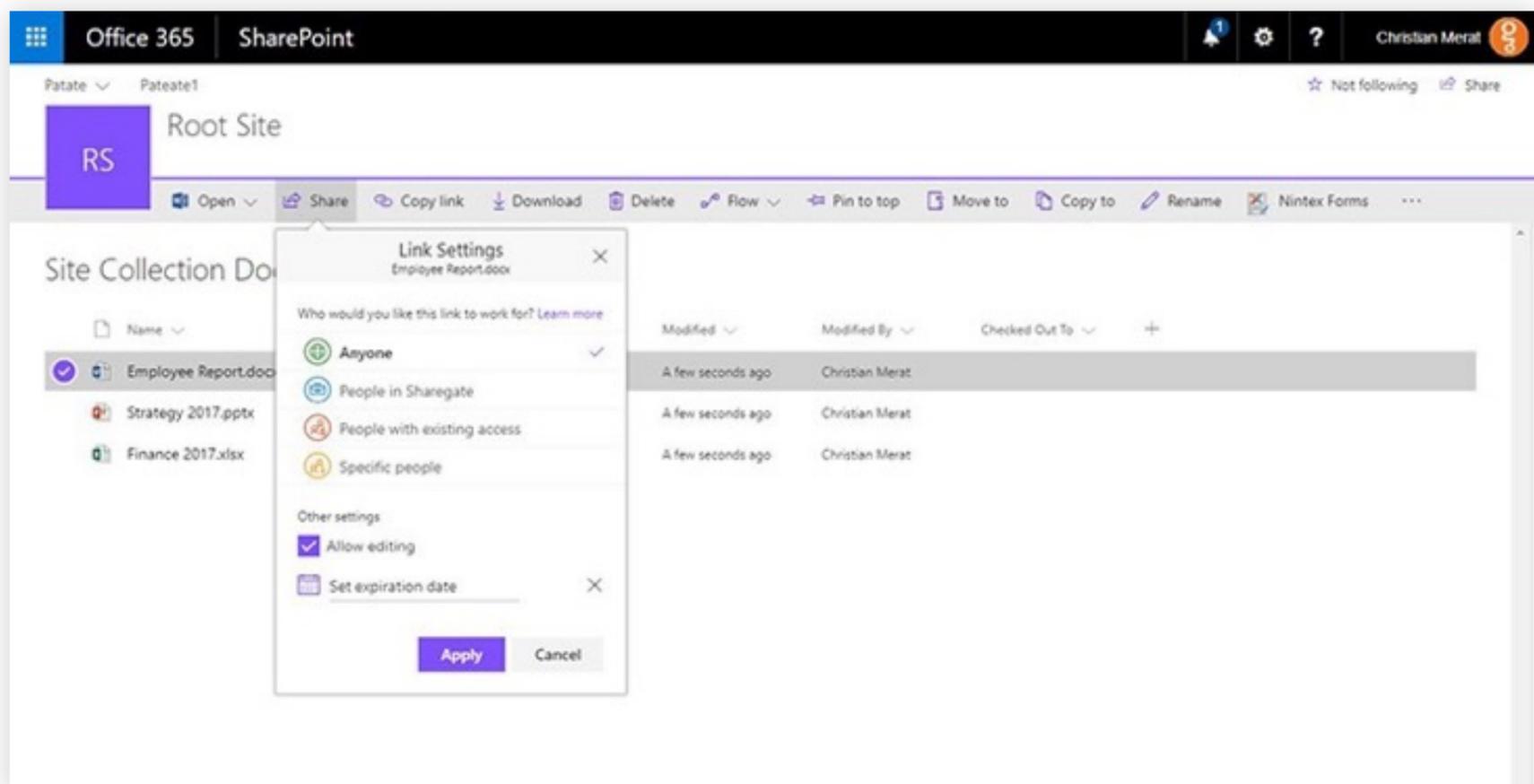
Depending on how external sharing has been configured, users have a few different options when they decide to share with people outside of the organization. As mentioned above, they can choose to share content with anonymous external users or with authenticated external users.

Sharing a SharePoint or OneDrive for Business Documents or Folder with an Anonymous User

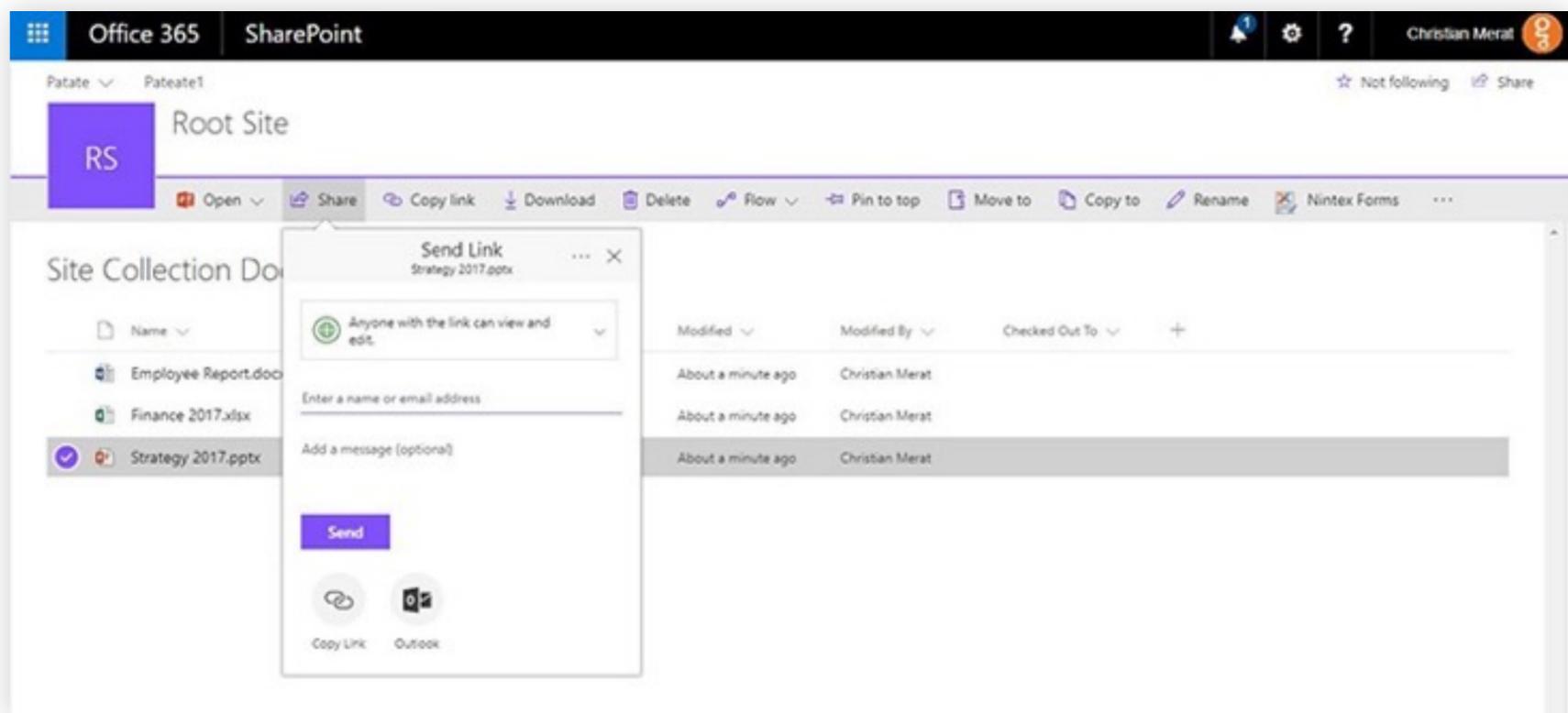
1. Go to the SharePoint document library or your OneDrive for Business in which the document or folder you want to share is located and select it by checking the circle on the left of the document title.



2. Click "Share" and "Anyone" in the link settings. You can choose to allow whether guest users can edit the document, and set an expiration date on the link.



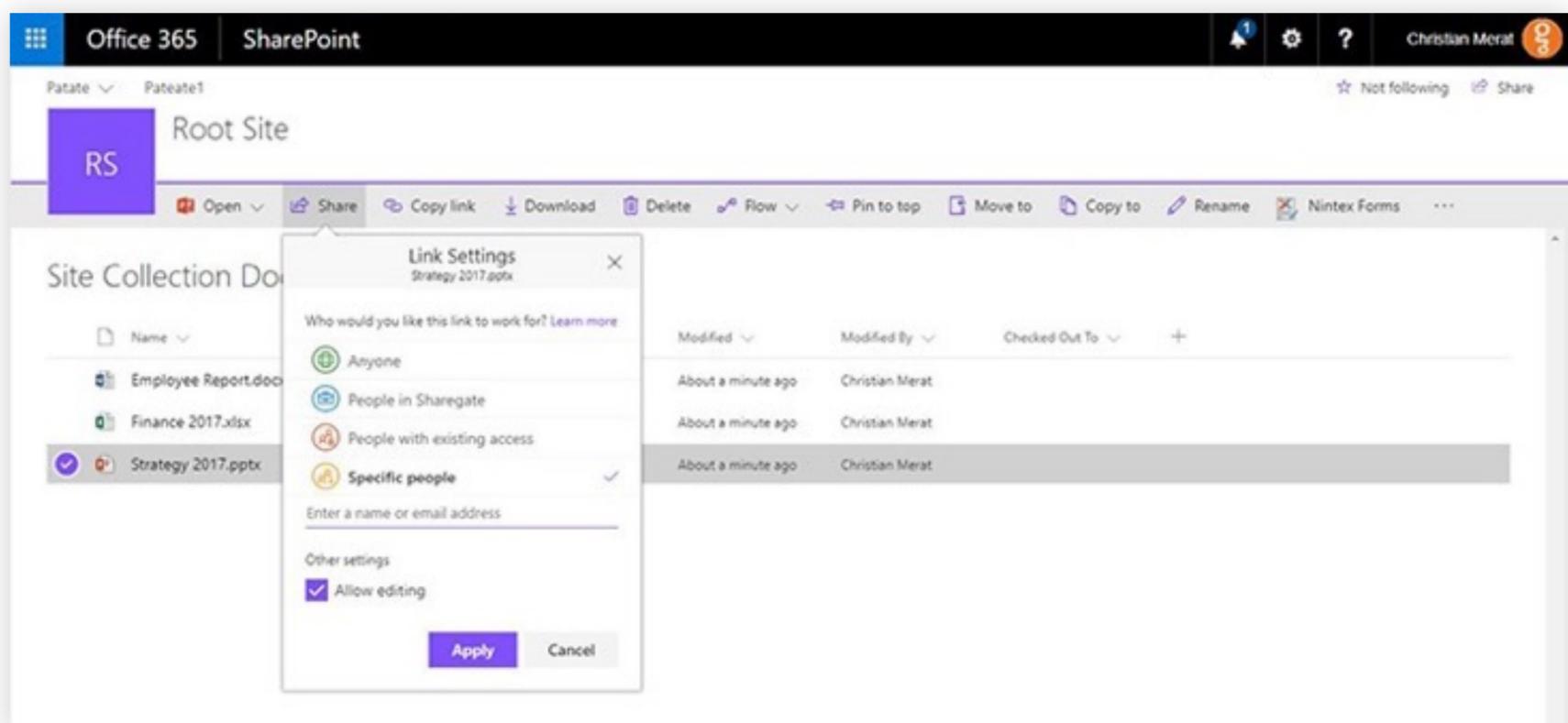
3. Once you've clicked "Apply," a link will be generated that you can then copy to your clipboard, or send via email. In this case, the email is only to send the link to your external user. It won't require them to log in to view documents.



Sharing a Document with an Authenticated External User

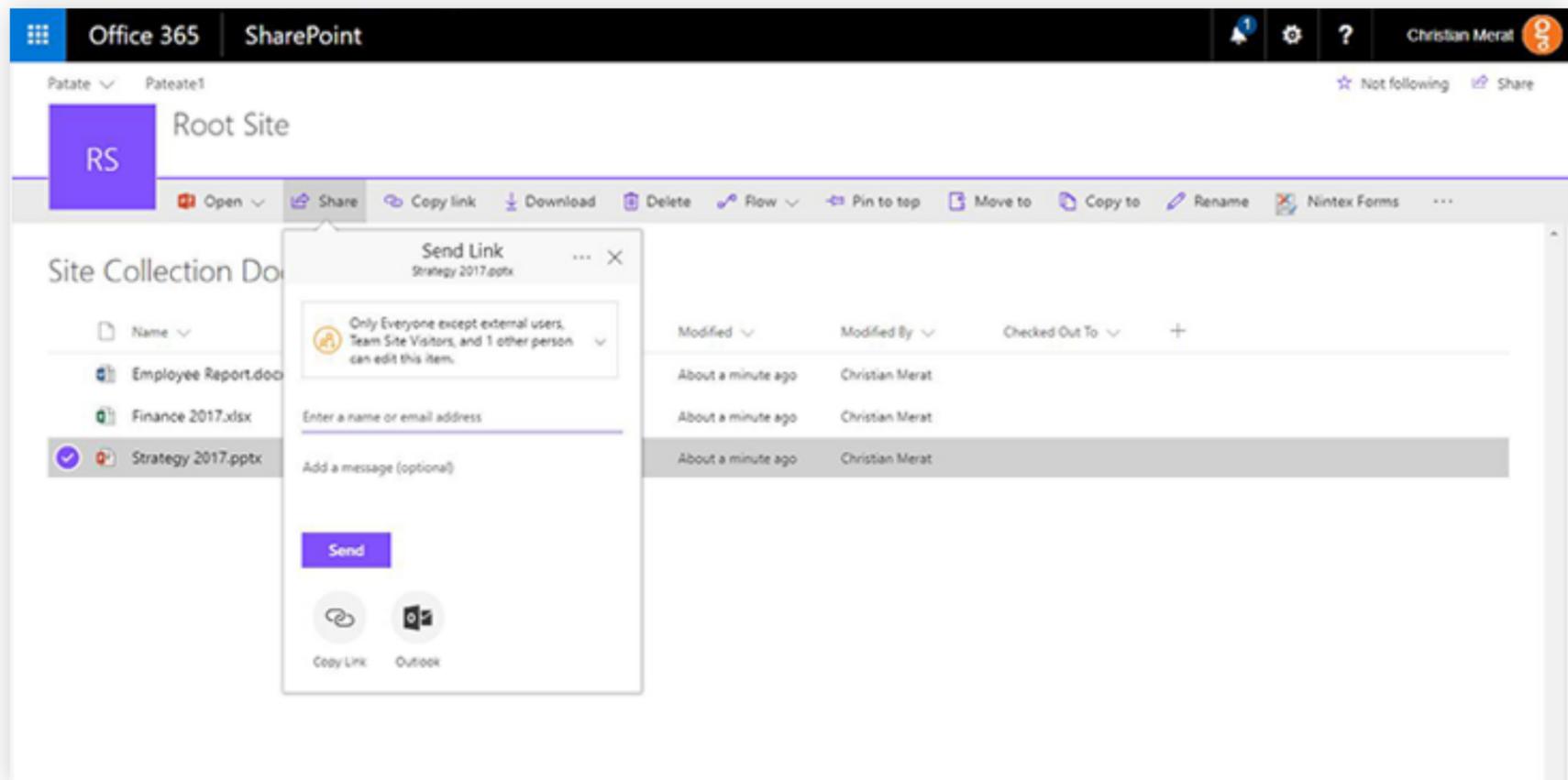
1. Sharing a document or folder with an authenticated external user is just as simple as creating an anonymous link. In the link settings, choose the "Specific people" option and type out the email address of the user you want to share your document with.

Just like with anonymous links, you can choose to allow whether guest users can edit the document, and set an expiration date.

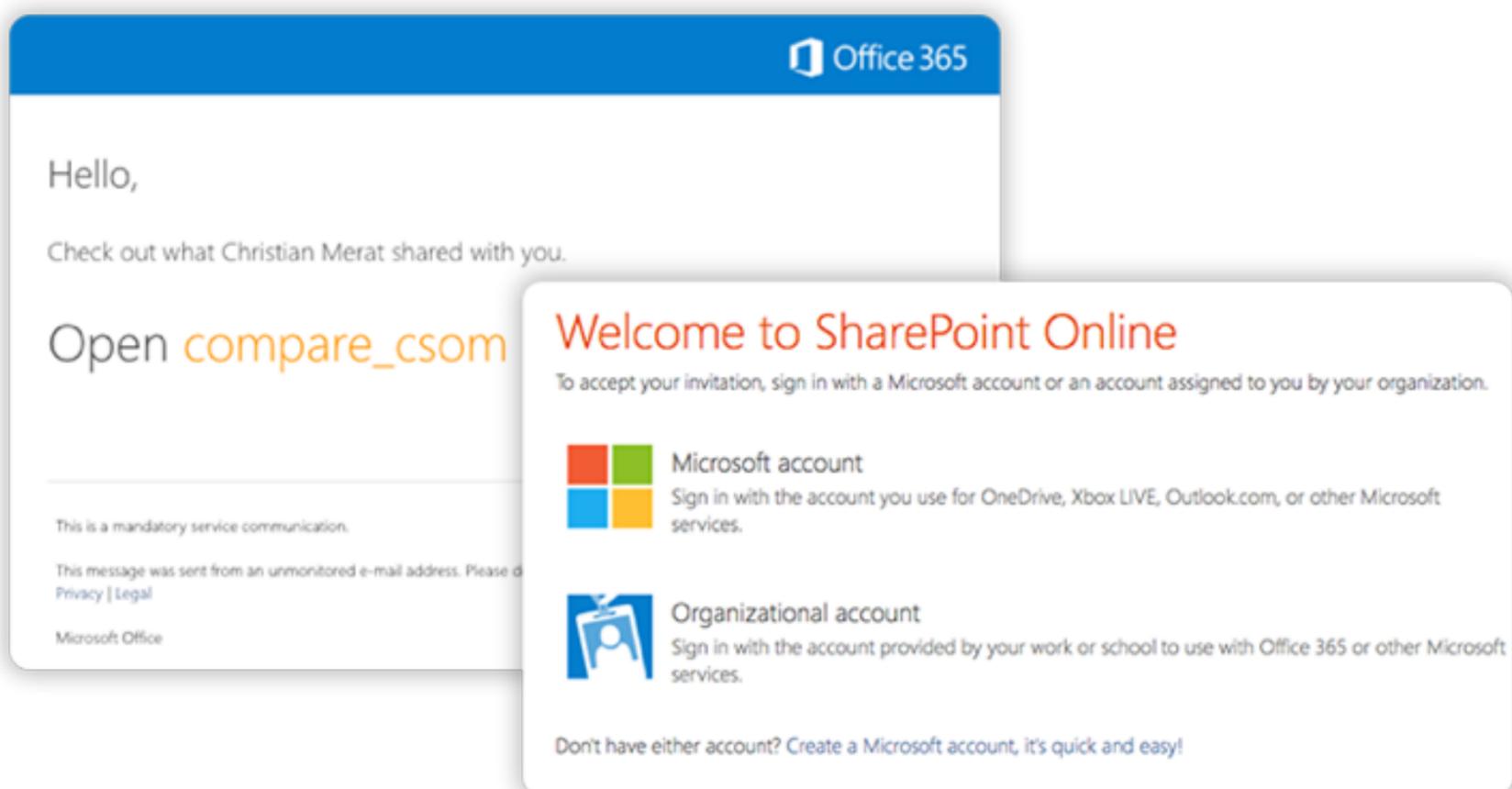


The other two options under "Anyone" are options for sharing a document with users already in your organization's directory.

2. Once you've clicked "Apply," you can choose to copy the link to your clipboard or to send it via email. Only the people you've invited specifically will be able to access the document. You'll also be able to see exactly who currently has access to the document.

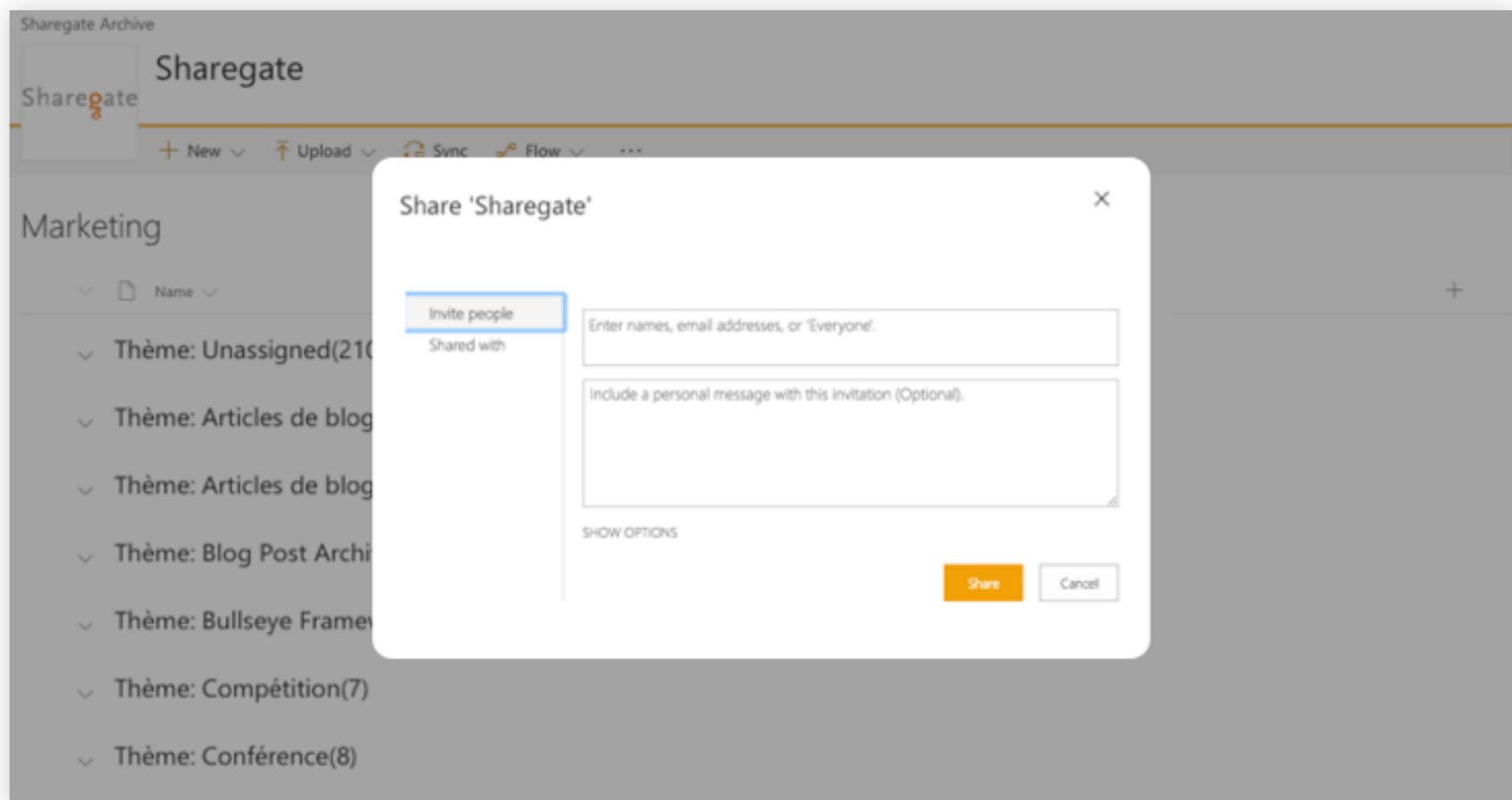


3. An invitation to join the document will be sent the guest user, who will have to accept it. Once accepted, they can log in using a trusted email address and he or she will be added to the organization's directory.

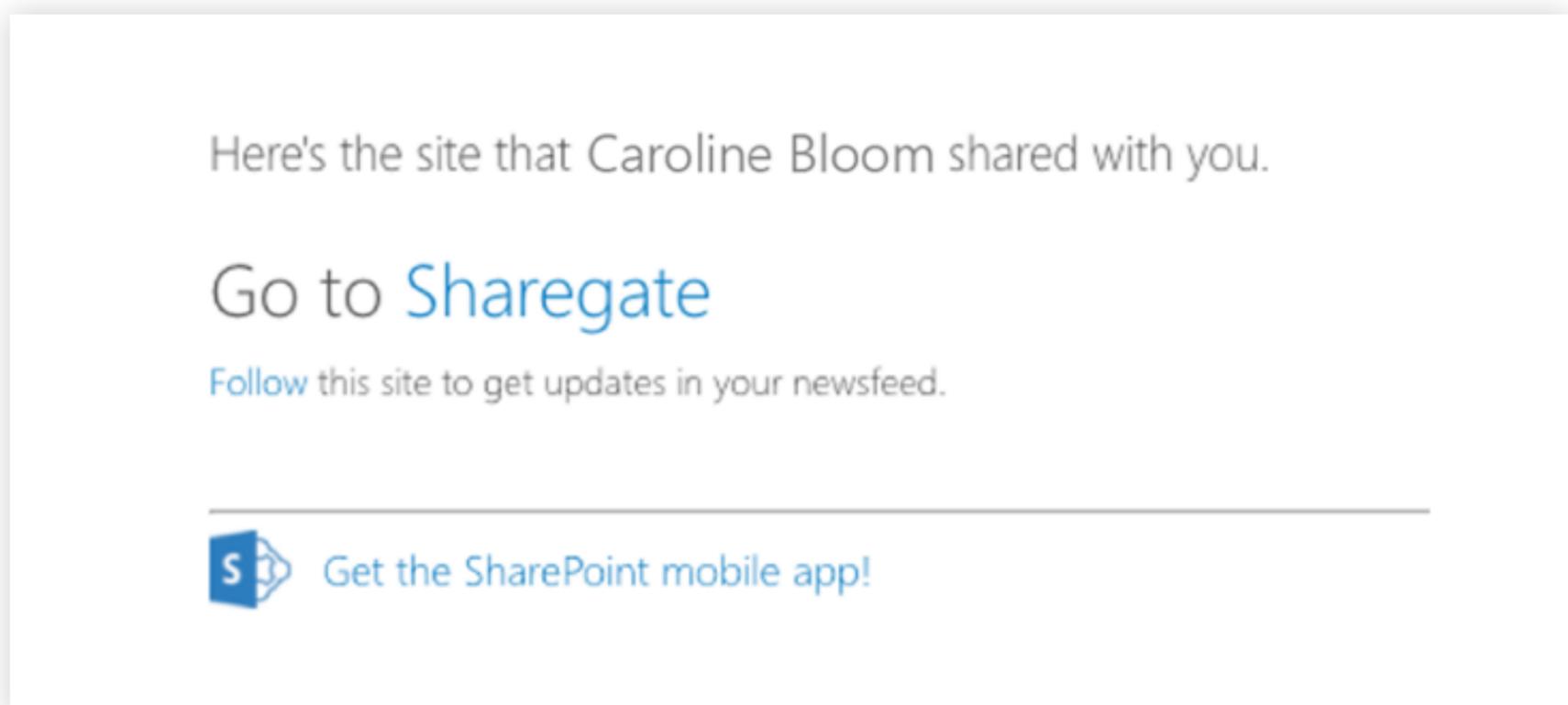


Sharing a SharePoint Site with Authenticated External Users

1. Sharing an entire SharePoint site with an external authenticated user works almost in the same way. Access the site in question and click the "Share" button in the top right-hand corner of the site.
2. In the popup window, type out the email addresses of the users you'd like to invite to your site.



3. The users will receive an invite to log in and access the site. As with sharing documents, if the user accepts the invitation, he or she will be added to your organization's directory.



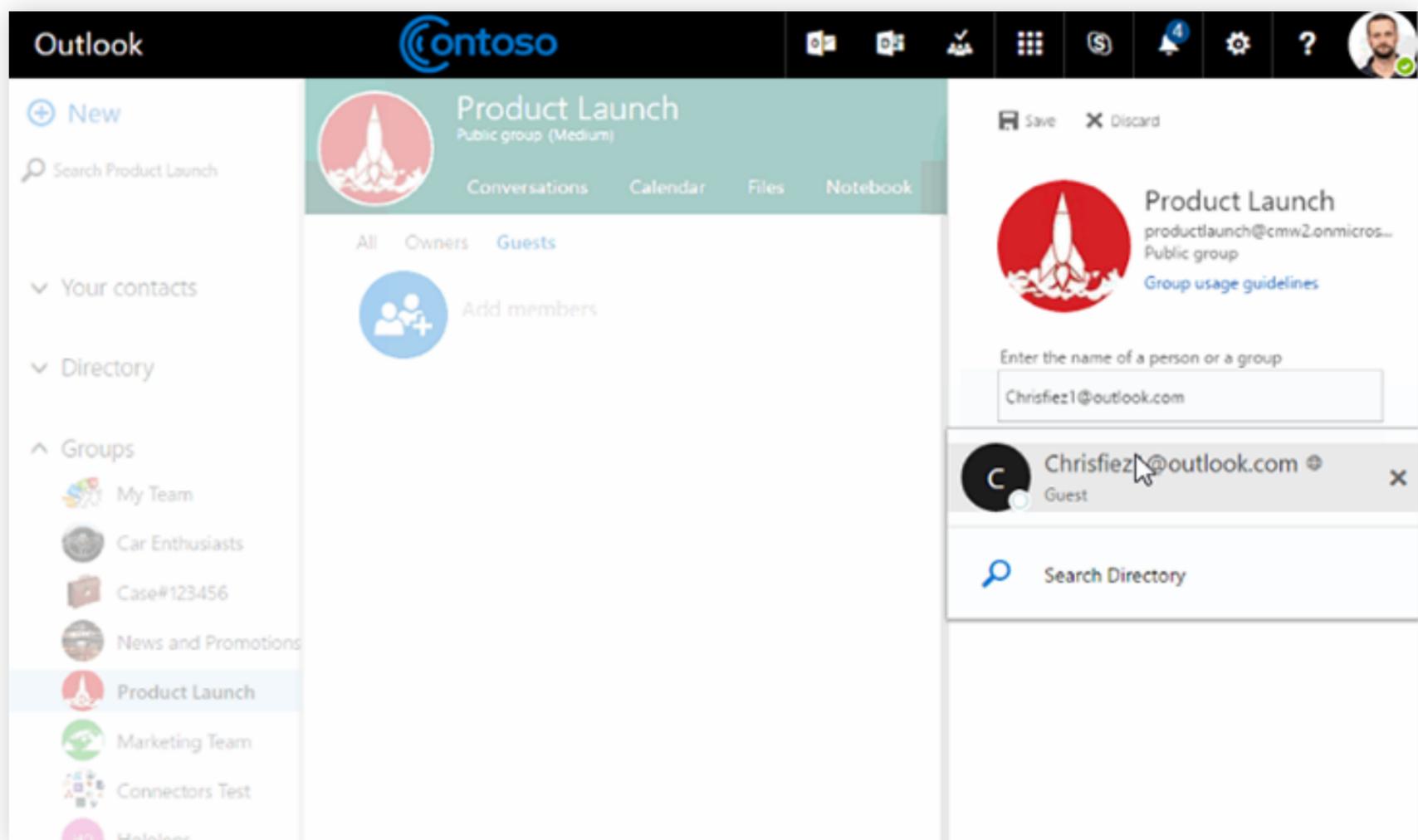
Adding a Guest User in Office 365 Groups

Another way of collaborating and sharing with an external user is by adding a guest user in an Office 365 Group.

It's essentially the same thing as adding an authenticated external user, so an invite will be sent to them via email, from there they will sign in with a Microsoft Account and a new guest user will be created in your Azure Active Directory.

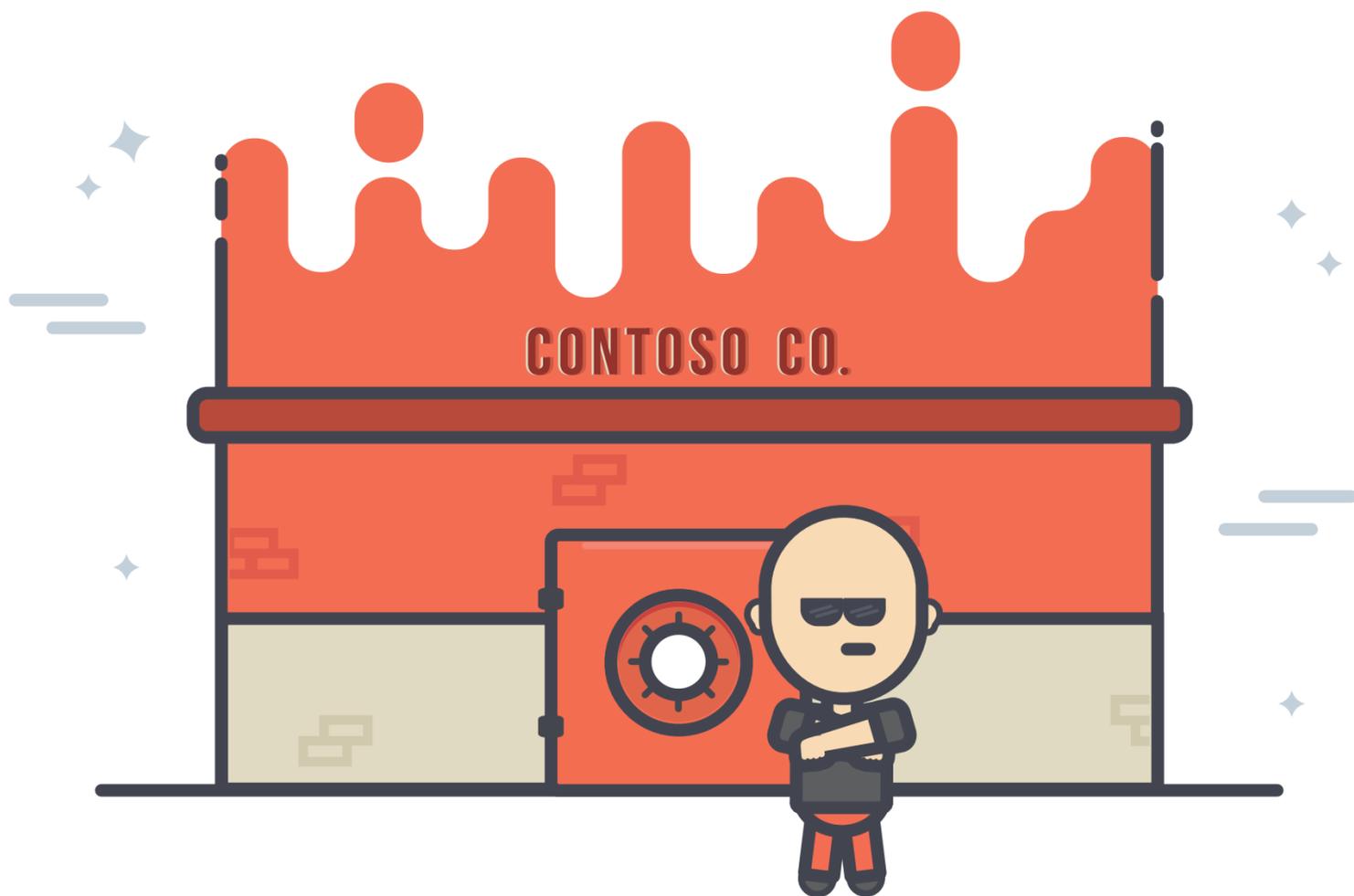
The main difference is that once the invitation accepted, they will receive all group emails, calendar invites, Yammer discussions, etc. and have access to the group's SharePoint Online Site and all its files.

When added as an Office 365 Group Member, they will automatically have complete control over the SharePoint workload, at all times. If you want to give them a more fine-grained access, then it's important to do it via SharePoint only, and not add them to the Office 365 Group.



CHAPTER FOUR

How To Manage External Sharing



If you're going to open up access to your environment to external users, it's important you stay aware and in control. As mentioned earlier, blocking all access out of fear will not necessarily solve the problem, the internet is full of solutions today. So how can you manage external sharing?

There are a few options you can look into:

- Configuring the right options for you in the Admin Center
- Managing External Sharing via PowerShell Commands and Scripts
- Using Sharegate Online

Managing External Sharing with the Admin Center

There's a number of options we discussed above when configuring this feature. Some of them can help you control access to your environment a little more, should you need to.

- Set default expiration links for all anonymous links created, always.
- Limit external users by their domain. You don't want invitations sent to Gmail accounts? Make sure only certain approved domains can enter or, the other way around, blacklist certain domains.
- Enforce that only a user with the same email address as the one the invitation was sent to can accept and sign in. The default behavior allows the recipient of the external sharing invitation to forward it to anyone else.
- Make sure external users can't share with others documents they didn't create.
- Dive into Device Access management and Intune to make sure only certain IP addresses are accepted, and enforce policies such as the blocking of the "Print" button on Office documents.
- Leverage the Azure Portal's access to your Azure Active Directory to see and manage your guest users throughout your Office 365 environment.

Managing External Sharing with PowerShell

This will require you to roll up your sleeves and dive into the world of Shell. You can write commands to query and find things like external users, as well as set certain options. At this point, it's up to you and your PowerShell expertise.

Managing External Sharing with Sharegate Online

Third-party tools can be extremely beneficial when managing and monitoring external sharing. [Sharegate Online](#) allows you to receive alerts whenever content is shared outside of your environment, either anonymously or with authenticated external users.

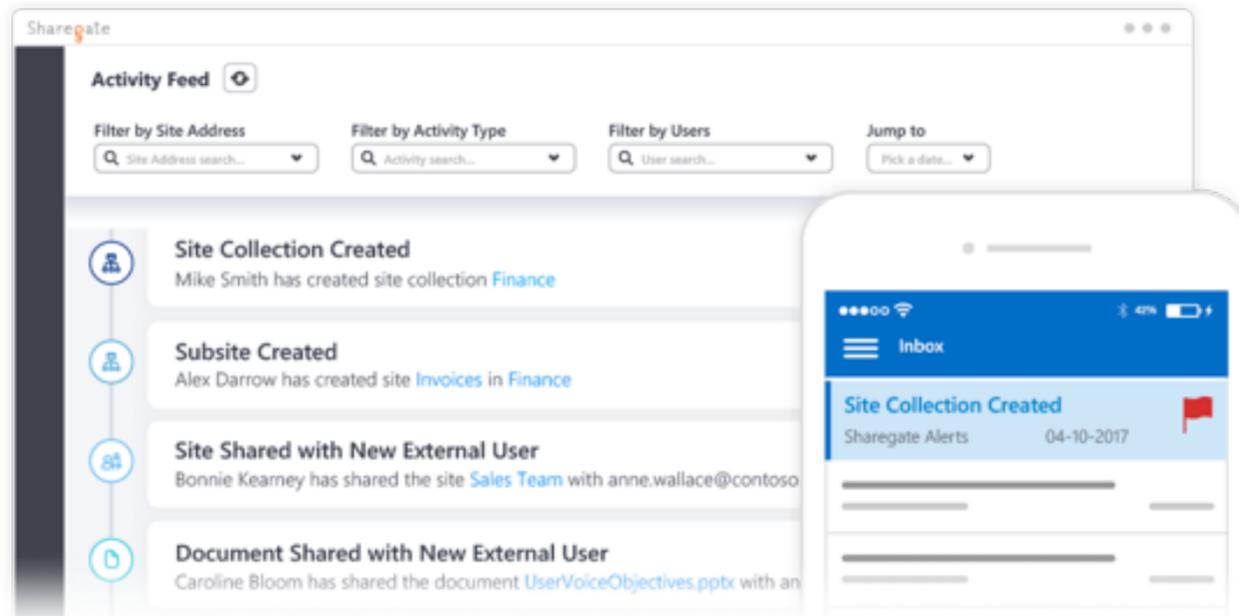
Also, all external activity will be aggregated in an activity feed, available on your dashboard. You'll gain a level of visibility that you wouldn't get otherwise.

External Sharing Best Practices

1. Don't turn off external sharing! Rather, configure external sharing to your specific business needs, while keeping in mind that your users will need to collaborate with external guests.
2. Implement proper governance policies to ensure everyone is on the same page when it comes to reacting to and correcting an external sharing blunder.
3. **Educate your users** on proper external sharing (i.e. how to share a document, vs. sharing a site) to avoid them inadvertently giving access to sensitive data.
4. In most cases, it's probably best to turn off anonymous sharing and only allow authenticated external users, or to set an expiration date at the very least. You'll be able to control and follow-up with who has access to what.
5. Double check the permission levels of your site collections to ensure external users don't inherit permissions that allow them to wreak havoc in your environment.
6. Manage security by checking reports every day.
7. Use third-party tools like **Sharegate Online** to receive alerts that help you keep track of content and understand what is shared outside of your company, and by whom.

External sharing can be a very important part of proper collaboration in your organization, so don't be afraid of it! Once you've understood the way it works, you'll never want to work any other way.

Gain Visibility, Control and Protect Your Office 365



Sharegate Online helps you gain visibility and control over usage in your Office 365 environment, by facilitating the detection of security anomalies, controlling what is shared outside your organization and helping to enforce governance plans.

Alerts

You'll be instantly notified when certain actions are performed:

- When a Site, a Document or a Document Library is shared externally
- When a Site Collection, Site or Subsite is created
- When an Office 365 Group is created
- And much more.

Activity Feed

- Displays all user activities and reveals which users are accessing sensitive data.
- Capture and investigate an audit trail of all user and administrator activities.

[Try Sharegate Online](#)

[Learn More](#)



About Sharegate

Sharegate makes it easier for organizations to adopt and use the latest Microsoft productivity tools, helping millions of users be happier and more productive at work.

Want to learn more?

Connect with us on twitter and visit **share-gate.com** for more SharePoint & Office 365 related content.



@sharegatetools



www.share-gate.com