Microsoft

Technical Guide

Microsoft 365 Collaboration Blueprint for UK Government

Prepared for UK Government - OFFICIAL

03 April 2023

Version 1.1

Prepared by

Microsoft Industry Solutions

Table of Contents

1 Introduction

1.1 Intended Audience

Technical staff responsible for the configuration and deployment of Microsoft 365 (MICROSOFT 365) services across UK government departments.

Security staff responsible for securing and monitoring information sharing.

1.2 Document Purpose

This document represents the 'Technical Guide' for the *Microsoft 365 Collaboration Blueprint for UK Government*. It outlines the configuration settings to enable effective collaboration across government organisations using key elements of Microsoft 365. It is accompanied by a 'Strategy' document outlining the technologies involved, why this approach has been taken and how it is secure
This document contains Microsoft 365 configuration guidance developed by the Central Digital and Data Office and Microsoft. The guidance was developed to allow easier and more consistent collaboration between government organisations using Microsoft 365 services.

The configuration forms a baseline set of security and collaboration standards, plus optional settings where appropriate, that aim to allow HMG organisations to collaborate with a common level of trust.

1.3 How to use this document

The Collaboration Blueprint should be adopted alongside other key technical guides for government organisations working in Microsoft 365:

1. The Microsoft 365 UK Blueprint - Secure Configuration Alignment was produced by Microsoft and the NCSC and updated in April 2021. It should be implemented as a secure foundation on which to adopt the *Collaboration Blueprint*.
2. Microsoft 365 UK Blueprint – BYOD Access Patterns was developed by Microsoft and the NCSC to help improve security for Bring Your Own Device use cases. For the vast majority of organisations this guidance is applicable due to the evolving nature of device management.

This document contains three main sections:

- Section 2: Baseline Microsoft 365 Configuration for Collaboration in UK Government – contains the actual configuration settings to be applied.
- Section 3: MICROSOFT 365 Security Considerations - contains information about security and monitoring.
- Section 4: Optional Configuration - contains information on optional configuration for certain capabilities. These items are not essential to align to the Collaboration Blueprint, however organisations may find benefits in implementing them.

Links to Microsoft "How to" guides are included so you can use these to apply the settings specified in the configuration section.

1.4 License Dependencies

The baseline configuration requires a minimum of Microsoft 365 E3 and Azure AD P2 licensing.

The optional component, Insider Risk Management requires E5 licencing, or E3 plus either E5 Compliance add-on or E5 Insider Risk Management add-on.

Device monitoring and alerting is available with E3 Enterprise Mobility or E5.

2 Baseline Microsoft 365 Configuration for Collaboration in UK Government

The baseline configuration described in this section should be applied to your tenants as it represents the minimum standards for Cross-Government Collaboration.

You may choose to leave your existing settings in place where existing settings enable equivalent collaboration and security, and your users can:

- Seamlessly send instant messages
- Collaborate on files in both SharePoint and Teams
- Effortlessly schedule meetings by viewing other users' free and busy calendar availability

2.1 Organisation and Security Settings

2.1.1 External Collaboration Settings

Follow the guidance in these links, using the settings from the table below: Enable B2B external collaboration settings - Azure AD | Microsoft Docs and Allow or block invites to specific organizations - Azure AD | Microsoft Docs

Setting Name	Value
Guest User Access	Guest users have limited access to properties and memberships of directory objects
Guest Invite Settings	Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
Enable guest self-service sign up via user flows	No (If you are already using B2C capabilities, you should not change this setting)
Collaboration Restrictions	Allow invitations to be sent to any domain

Table 1 External Collaboration Settings

2.1.2 Cross-Tenant Access

Cross-tenant access settings provide greater assurance and more control over B2B sharing between tenants.

We recommend using cross tenant access settings (XTAS) over tenant restrictions (TR) for collaborating across tenants. While TR does not support the default sharing approach recommended in this Blueprint, which allows documents to be shared using modern

collaboration approaches instead of defaulting to email, XTAS provides more granular control over the business-to-business (B2B) relationship between two organizations.

With XTAS, you can make applications available to specific groups of users and use multi-factor authentication (MFA) and device state as part of the access decision when accessing documents. TR limits the external tenants that can be collaborated with, while XTAS allows for a more flexible and secure approach to collaborating across organizations.

There are three types of control available:

Control	Description
Inbound Access Settings	Allows you to control which users in a remote tenant can be guested into your organisation, based on group membership in the remote tenant. Allows you to control which applications can be accessed by guest users from the remote tenant
Outbound Access Settings	Allows you to control which of your users can collaborate with the remote tenant. Allows you to control which applications in the remote tenant can be accessed by your users
Trust Settings (Inbound only)	Allows your tenant to accept MFA and Device Compliance claims from the remote tenant

Table 2 Cross-tenant Access Settings overview

You can configure default settings for your organisation and configure settings per external organisation.

To establish trust settings for another organization's device compliance claim, the external organization must use a Mobile Device Management (MDM) product such as Intune or a 3rd party product that can report device compliance to Azure AD for use in evaluating conditional access policies.

You should speak to your partner organisation’s technical team to understand their device management posture before enabling device compliance trust settings.

If an organisation does not have an MDM solution that supports device compliance claims in AAD, consider enabling Hybrid AAD Join trust settings for that organisation.

By enabling this trust, you can gain some confidence in the partner organisation's device by ensuring it is at least joined to their corporate IT system.

Enabling Hybrid Azure AD Join trust settings can also help organizations better collaborate with other organizations as it provides a means for on-premises devices to be included in device compliance evaluations, allowing for a more complete picture of device compliance across the entire environment.

2.1.2.1 Organisational Settings

Follow the guidance at this link using the settings from the table below: Configure B2B collaboration cross-tenant access - Azure AD | Microsoft Docs

For each organisation you want to control sharing for, click Add Organisation, enter the tenant name you wish to add then click save. Using the settings below, modify the trust settings to enable MFA and Device Compliance claims from the external organisation.

Setting Name	Value
Trust Settings	Customize Settings
Trust multi-factor authentication from Azure AD tenants	Ticked
Trust Compliant Devices	Ticked
Trust hybrid Azure AD joined devices	Unticked

Table 3 Cross-tenant Access Configuration Settings

By default, organisations for whom you have no relationship configured are not trusted for MFA, Device Compliance and Hybrid Joined Device claims.

2.1.3 Conditional Access Policy for Guest Users

Follow the guidance in these links, using the settings from the tables below: Terms of use - Azure Active Directory | Microsoft Docs and Create a secure guest sharing environment | Microsoft Docs

Upload your organisation's Terms of Use to Azure as part of your configuration. Setting	Value
Name	Baseline Guest Terms of Use
Display name	Baseline Guest Terms of Use
Terms of use document	Upload the relevant PDF file and select a language. Additional PDF files in other languages can be added if required
Require users to expand the terms of use	On
Require users to consent on every device	Off
Expire Consents	On
Expire starting on	Choose some future date

Upload your organisation's Terms of Use to Azure as part of your configuration. Setting	Value
Frequency	Annually
Duration before re-acceptance required (days)	30
Conditional access: Enforce with conditional access policy templates	Create conditional access policy later

Table 4 Terms of Use for Guest Users

Create a conditional access policy with the following settings:

Setting	Value
Name	Baseline Guest Access Policy
Assignments: Users and groups	Include Select users and groups All guests and external users
Cloud apps or actions	Include All cloud apps
Conditions	N/A
Access controls	Grant Access Require multi-factor authentication: Ticked *Baseline Guest Terms of Use* (or whatever you chose to name the terms of use object): Ticked Require all selected controls: Checked
Session	N/A
Enable policy	On

Table 5 Conditional Access Policy for Guest Users

This policy means that guest users will be required to complete MFA to access your data. If the user is from a tenant with whom you have a relationship configured in Cross-Tenant Access Settings and where you trust their MFA claims, they can use their MFA, and they will not be required to register for MFA in your tenant. In all other cases, this policy will require users from external organisations to register for MFA in your tenant.

This policy means that guest users will be required to accept a terms of use document when they log in.

If users from external organizations do not complete MFA registration, access to your tenant will be denied in accordance with this policy.

2.1.4 One-time Passcode Authentication

Review one-time passcode authentication settings and turn it on if it isn't already. Follow the guidance at this link: [One-time passcode authentication for B2B guest users - Azure AD | Microsoft Docs]

Ensure that you set 'Enable email one-time passcode for guests effective now' if that option is available in the portal.

OTP is a pre-requisite for SharePoint B2B integration detailed in 2.3.2.

2.1.5 Anonymous calendar sharing

This setting prevents anonymous third-party users from viewing calendars, which may include meeting links and other sensitive information.

Follow the guidance in the link, using the settings from the table below to turn off anonymous calendar sharing: [Share calendars with external users - Microsoft 365 admin | Microsoft Docs , since this setting is in the secure configuration alignment, make sure it is unticked.]

Setting	State
Allow anyone to access calendars with an email invitation	Unticked

Table 6 Calendar sharing settings

2.2 Microsoft Teams

2.2.1 Guest Access Settings

Follow the guidance in the link, using the settings from the table below: [Microsoft 365 guest sharing settings reference | Microsoft Docs]

Microsoft 365 Admin Center > Settings > Org Settings > Security & Privacy > Sharing

Setting	Value	Impact
Let users add new guests to the organisation	On	Azure AD members can invite guests via Azure AD, or MICROSOFT 365 Group members can invite guests with owner approval

Table 7 Guest access sharing settings

Microsoft 365 Admin Center > Settings > Org settings > Microsoft 365 Groups

Setting	Value	Impact
Let group members outside of your organisation access group content	On	This setting should be **On** for *any* scenario where guests are interacting with MICROSOFT 365 Groups or Teams The setting must be on to allow guests to interact with Teams because it grants them necessary permissions and access to participate activities and collaborations
Let group owners add people outside your organisation to groups	On	Owners of Microsoft 365 Groups or Teams can invite new external guests

Table 8 Guest access group settings

Teams Admin Center > Users > Guest access

Setting	Value	Impact
Calling – Make Private Calls	On	This enables guest users to make peer-to-peer calls from your tenant.
Meeting – IP Video	On	This enables guest users to make video calls from your tenant
Meeting – Screen Sharing Mode	Entire Screen	Entire Screen will share a whole screen, regardless of what applications are running or moved to it Single Application will just share one application. **The choice between these is determined by the sensitivity of your environment.**
Meeting – Meet Now	On	This enables the "Meet Now" button to be active in Teams and facilitates collaboration.
Messaging – Edit Sent Messages	On	Allows guests to edit messages which have been sent.
Messaging – Delete Sent Messages	On	Allows guests to delete messages which they have sent. **Note**: You may not wish to allow guests to delete their messages if you need to keep them for record information.
Messaging – Delete Chat	Off	Prevents guests from deleting the entire chat.
Messaging – Giphy in conversations	On	Enabling this permits the use of GIFs in conversations
Messaging – Giphy Content Rating	Strict	This setting will only allow GIFs which are safe for work.
Messaging - Memes in conversations	Off	Off – Memes cannot be shown
Messaging – Stickers in conversations	On	On – Stickers can be shown
Immersive reader for messages	On	A setting of on enables the immersive reader functions, which is an accessibility feature

Table 9 Guest access settings for meetings

2.2.2 External Access

Follow the guidance in the link, using the settings from the table below: Manage external access (federation) - Microsoft Teams | Microsoft Docs

Teams Admin Center > Users > External access

Setting	Value
Teams and Skype for Business users in external organisations	Block only specific external domains

Table 10 Teams external access settings

2.2.3 Teams Settings

Follow the guidance in the link, using the settings from the table below: Manage settings for your organization - Microsoft Teams | Microsoft Docs

Unless there is a business need, you should prevent your users from uploading data to other cloud data storage services.

Teams Admin Center > Teams > Teams settings > Files

Setting	Value
Citrix files	Off
DropBox	Off
Box	Off
Google Drive	Off
Egnyte	Off

Table 11 Teams file sharing settings

2.2.4 Meeting Settings

Follow the guidance in the link, using the settings from the table below: Manage meeting settings - Microsoft Teams | Microsoft Docs

Teams Admin Center > Meeting Settings

Setting	Value	Impact
Anonymous users can join a meeting	On	When set to on, this allows participants who do not have an AzureAD login to join a meeting.
Anonymous users can interact with apps in meetings	On	This enables participants who do not have an AzureAD login to interact with apps in meetings, providing a collaborative experience.

Table 12 Teams meeting settings

You should allow anonymous users to join meetings, otherwise you will prevent non-Microsoft 365 organisations from joining meetings.

2.2.5 Meeting Policies

Follow the guidance in the link, using the settings from the table below: [Teams: Manage meeting policies - Microsoft Teams | Microsoft Docs]

Teams Admin Center > Meetings > Meeting Policies > Global Meeting Policy > Participants and Guests

Setting	Value	Impact
Let anonymous people start a meeting	Off	This ensures external participants are placed in the lobby until admitted by a presenter.
Roles that have presenter rights in meetings	Everyone in the organisation, but the user can override	This prevents guests from having the ability to mute participants and other interactive features unless explicitly given Presenter rights during the meeting.
Automatically admit people	People in my organization	This ensures participants outside of the organisation are added to the lobby and must be admitted to the meeting by a presenter. This provides a level of validation that attendees are authorised by a member of the hosting organisation.
Allow dial-in users to bypass the lobby	Off	This secures the environment but does mean that dial in parties externally and internally will be held in the lobby.
Meet now in private meetings	On	This facilitates collaboration through the "Meet now" functionality and enables impromptu private meetings.
Live Captions	Not enabled but the user can override	This allows individual users to turn on captioning if required
Chat in meetings	Enabled	This is helpful not only for sharing information, but also for accessibility.

Table 13 Teams meeting policies

2.3 SharePoint Online

2.3.1 SharePoint Policies

Follow the guidance in the link, using the settings from the table below: [Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Docs]

SharePoint Admin Center > Policies > Sharing

Note: Limiting external sharing will prevent collaboration with external users using public email services (e.g. Gmail users).

Expand the "More external sharing settings" menu to see all the settings.

Setting	Value	Impact
Limit external sharing by domain	Off	This enables users and guests to share with anyone from any domain.
Allow only users in specific security groups to share externally	Off	Unless there is a pressing organisational requirement to restrict certain parties' ability to share information, it is recommended to leave this off.
Guests must sign in using the same account to which sharing invitations are sent	On	This ensures that only the intended party is opening the shared document.
Allow guests to share items they don't own	On	This provides a cohesive collaborative experience for guest users, however depending on organisational risk appetite, it could be turned off. When set to Off, guests can only share items which they have created.
Guest access to a site or OneDrive will expire automatically after this many days	30	Guests will lose access to documents, folders or sites shared with them after 30 days. If you want guests to have long term access to shared information, set a suitable expiration period for the site, or use a Teams site, or site connected to a MICROSOFT 365 group.
People who use a verification code must reauthenticate after this many days	14	This relates to information shared with non-guests who have authenticated with One Time Password (OTP)
File and Folder Links	Only people in your organisation	This sets the default behaviour in the share dialogue in SharePoint and in office documents. The user can choose to share with specific people to enable ad-hoc sharing
Choose the permission that's selected by default for sharing links	Edit	This sets the default behaviour in the sharing dialogue to Edit. The user can choose to apply "view only" and "block download" controls if they wish
Show owners the names of people who viewed their files in OneDrive	On	This enables file owners to see the names of people who have viewed their files.
Let site owners choose to display the names of people	On	This enables SharePoint site owners to see the names of people who have viewed their files.

Setting	Value	Impact
who viewed files or pages in SharePoint		
Use short links for sharing files and folders	On	This shortens the sharing link and provides a more friendly URL

Table 14 SharePoint sharing settings

2.3.2 Enable Azure AD B2B integration for SharePoint and OneDrive

For more details, see Azure AD B2B integration for SharePoint & OneDrive - SharePoint in Microsoft 365 | Microsoft Docs

You must have configured one-time passcode authentication, as described in 2.1.4 before enabling this integration.

To enable SharePoint and OneDrive integration with Azure AD B2B:

Step	Action
1	Download the latest SharePoint Online Management Shell **Note:** If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
2	Open SharePoint management shell from the start menu and connect to SharePoint online using the following command: Connect-SPOService -Url https://*tenantName*-admin.sharepoint.com -Credential '*GA or SharePoint Admin credentials*'
3	Run the following cmdlets: Set-SPOTenant -EnableAzureADB2BIntegration $true Set-SPOTenant -SyncAadB2BManagementPolicy $true

Table 15 Enable SharePoint and OneDrive integration with Azure AD B2B

2.4 OneDrive for Business

2.4.1 Sharing

Follow the guidance in the link, using the settings from below: Control notifications - OneDrive | Microsoft Docs

SharePoint Admin Center > Settings > OneDrive Notifications

Tick "Allow notifications"

2.5 Exchange Online

2.5.1 Message Filtering

Collaboration invitations are sent in HTML format. To preserve the formatting of the email and the message content, mail clients must be configured to be able to receive and show HTML format emails from authorised domains.

If users have added any entries to their Blocked Senders list in Outlook, then these will still be filtered out. It is also possible to configure users' Safe Senders list in Outlook to enable more reliable delivery of email as referenced in Configure junk email settings on Exchange Online mailboxes - Microsoft 365 | Microsoft Docs

You should configure your spam filters to ensure that genuine emails are delivered to your end users. This is particularly important for notifications such as Sharing Links and Teams invitations, which users may miss if they are delivered to their junk email folder. Microsoft do not maintain a list of senders for these notifications as they can change over time. Your users should report when important notifications are delivered to junk so that you can update your allow lists accordingly.

2.5.2 Organisational Relationships for Calendar Free/Busy Sharing

To enable calendar availability sharing with other organisations, you need to complete these steps:

- Create an organisational relationship in your own Exchange Organisation.
- Create an organisational relationship in the other Exchange Organisation.
- Configure the level of calendar access for different domains or users using sharing policies.

Follow the guidance in the link, using the settings from the table below: Create an organization relationship in Exchange Online | Microsoft Docs

Caution: You should avoid doing the following which may prevent the calendar availability sharing from working correctly:

- Creating a duplicate organization relationship for the same domain.
- Removing the onmicrosoft.com domain from the configuration.
- Enabling free/busy information access for individual users instead of using sharing policies.

Setting	Value	Impact
Relationship Name	Value of choice	This is the name of the policy e.g. "Sharing with HMG"
Domains to share with	List of HMG domains	You cannot use wildcards, e.g., *.gov.uk, in the "Domains to share with:" field. Where an organisation has multiple domain names registered to a tenant, you only need to enter **one** of those names. The system will discover any additional domain names associated with the tenant.
Enable calendar free/busy information sharing	Ticked and option box: Calendar free/busy information with time only	Share free/busy calendar information only with no further subject or location information
Share calendar free/busy information for:	Everyone in your organisation	Enables free/busy calendar sharing for everyone. An individual policy can be defined for users who you want to restrict, or individual users can change the sharing default for themselves.

Table 16 Calendar sharing settings

> Note: It's also possible to configure organizational relationships using PowerShell. See section 4.5.1

2.5.3 Restricting calendar sharing

If there is a requirement to override the sharing of availability details for certain individuals in a controlled manner, a department can restrict calendar sharing of certain mailboxes.

There are two methods to achieve this:

1. Select the option "A specified security group", and then add all other security groups who you wish to have sharing capability, omitting the security group which you would wish to remain private.
2. Configure an individual sharing policy for VIP's and assign the policy to the individuals as default. This will prevent the federated organisational sharing, but still allow them to share their calendar both internally (up to and including delegate permissions) and externally as only free/busy.

Individuals may also limit their own sharing of availability details by using the options available in the Outlook app. Setting the organisation sharing level to 'None' achieves this.

Individuals should not share their calendar over the internet with third party individuals who are not part of a government department unless there is a valid business justification in accordance with their organisation's policy.

Create a sharing policy in Exchange Online | Microsoft Docs

3 Microsoft 365 Security Considerations

This document does not detail specific security related settings to be configured in a tenant, since each organisation has its own security posture or requirements. However, there are certain areas that we recommend are considered.

3.1 Monitoring collaboration activities

Basic logging is available in Compliance Center as part of MICROSOFT 365 E3. In addition, E5 licensing brings access to more powerful and automated features such as Insider Risk Management and Defender for Cloud Apps. Configuration for these solutions is dependent on specific organisational requirements, risk posture and policies.

Integrate MICROSOFT 365 monitoring with Security Information and Event Management (SIEM) solutions (including Azure Sentinel) to provide alerts through a single pane of glass. SIEM server integration with Microsoft 365 services and applications - Microsoft 365 | Microsoft Docs

You can use the Microsoft Graph Security API to allow direct access to security events and to build custom alerting or integrations with existing solutions. Security solution integrations using the Microsoft Graph Security API - Microsoft Graph | Microsoft Docs

To monitor sharing activities, you can configure rules and alerts in MICROSOFT 365 Defender and MICROSOFT 365 Compliance:

1. **MICROSOFT 365 Defender** - You can configure policies to trigger alerts based on events. Examples are creating a sharing invitation for external users (which can be narrowed to include just certain site collections), suspicious sending patterns, malware removed, downloaded files, and many others. Also available is automatic alerts notifications to particular email addresses e.g. the SOC Team. You can enable logging and alerting for applications in Defender for Cloud Applications, and for devices in Defender for Endpoint. The features available depend on licensing. The capabilities available in the various plans can be found here: Microsoft Defender for Microsoft 365 service description - Service Descriptions | Microsoft Docs

2. **MICROSOFT 365 Compliance** – Enables extended audit log retention, together with much more sophisticated features related to information protection and governance, insider risk management, and discovery and response. Of particular interest, is Insider Risk Management, an overview of which is given below. The entire solution catalogue can be found Microsoft 365 solution catalog - Microsoft 365 Compliance | Microsoft Docs.

3.2 Insider Risk Management

Insider Risk Management provides tenant level tools to help monitor user activity. It requires E5 licencing, or E3 plus either E5 Compliance Add-on or E5 Insider Risk Management add-on. E3 Enterprise Mobility and Security provides device level alerts. These features allow more permissive collaboration while ensuring that user activities can be monitored and alerted on.

Get started with insider risk management - Microsoft 365 Compliance | Microsoft Docs

Set up alerts for the types of risk activities you want to detect and investigate. These could include "Removing sensitivity labels from SharePoint sites", "Downloading content from SharePoint" etc.

In addition, alerts can be used to influence user behaviour – for example an alert for "sharing attachments via email to recipients outside the organisation" can help encourage users to use links instead of attachments when sharing externally, thereby improving security.

Set up Intelligent Detections to monitor activity to unknown or untrusted domains. Allowed domains can be excluded from detection, which can help reduce false positives.

3.3 Email Security

NCSC offer extensive guidance on securing email services and preventing spoofing. Review and follow the guidance at this link: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing

Microsoft also issue guidance on implementing Sender Policy Framework (SPF) and DomainKey Identified Email (DKIM), which help to ensure that emails are 'security marked' so that spoofed email addresses are detected and appropriately dealt with: Microsoft 365: Using SPF, DKIM and DMARC for Secure Messaging - TechNet Articles - United States (English) - TechNet Wiki (microsoft.com)

Upstream filtering solutions (e.g., Proofpoint) must be configured to allow receipt of emails from the authorised list of domains.

4 Optional Configuration

This section details areas of configuration which are optional, or which build on the core configuration to provide enhanced capabilities or better security. You do not need to enable the following settings to align with the Collaboration Blueprint, but there may be benefits to your organisation in doing so.

They are either for features which are only available with certain licensing or where settings require consideration within the context of your environment and therefore cannot be prescribed within the baseline.

4.1 External Collaboration

4.1.1 Custom Terms of Use for Guests in Different Organisations

You can create custom terms of use depending on the organisation a guest user is joining from. Use a combination of Dynamic Groups and Conditional Access policies to scope ToU to specific sets of users.

The dynamic group membership should be based on the domain name for the guest user's organisation. In the case of an organisation having multiple domains associated with it, you need to make sure that all their domains are used as criteria for the dynamic group. Pay careful attention to dynamic group membership rules to ensure that only users from the desired organisations are added. For example, use "hmtreasury.gov.uk" instead of the word "treasury" to ensure that only users matching the full domain name are added to the group.

Full guidance for creating ToU and using Dynamic Groups to scope Conditional Access Policies can be found here: Terms of use - Azure Active Directory | Microsoft Docs.

Rules for dynamically populated groups membership - Azure AD | Microsoft Docs

4.1.2 Microsoft 365 Web Apps for Guest Collaboration

Security is one of the main reasons why we strongly suggest using Microsoft 365 Office Web Apps for guest collaboration.

Web Apps can be used to prevent guests from downloading or syncing files to their devices, which helps to safeguard sensitive information and prevent data breaches.

Sensitivity labels are built into Microsoft 365 Web Apps on Windows, macOS, iOS, and Android to provide users with a consistent labelling experience across these devices when using Microsoft 365 Web Apps.

4.2 Microsoft 365

4.2.1 Sensitivity Labels

Sensitivity Labels can be used to classify and protect documents and emails. They can also protect content in Microsoft Teams sites, Microsoft 365 Groups and SharePoint Sites. The addition of sensitivity labels supports your users with more ways to classify and control teams sharing. For example:

- Whether a Team is private or public
- Whether external users are allowed
- Allow or prevent external sharing
- Control access from unmanaged devices

Sensitivity Labels support the user to better handle information, by providing a visual indication in the Team and allowing them to apply security controls to shared items that cannot be overruled by end users.

An overview of sensitivity labels is available on Microsoft Docs Learn about sensitivity labels - Microsoft Purview | Microsoft Docs

The SharePoint site that underpins the Team still retains its original sharing setting and must be updated to match the Team. As an example, see Configure a team with security isolation | Microsoft Docs

4.3 Entitlement Management Settings

If you would like to make use of policies that ensure external users are removed from the directory after a set time to reduce the risk of stale external access, consider using Entitlement Management settings with an appropriate time period set for your organisation.

Follow the guidance in the link, using the settings from the table below: Govern access for external users in Azure AD entitlement management - Azure Active Directory | Microsoft Docs

Setting	Value
Block external user from signing into this directory	Yes
Remove external user	Yes
Number of days before removing external user from this directory	Specify a number of days

Table 17 Guest lifecycle settings for Entitlement Management

This setting only affects external users who are invited to the organisation through Entitlement Management Access Packages. It applies to users from all external organisations. It does not affect external users who are invited as guests through O365 apps directly. These settings will prevent such external users from logging in when they lose access to their access packages and will delete their guest accounts after the time period configured in this setting (default 30 days).

4.4 B2B Direct Connect

B2B Direct Connect is a pre-requisite for Teams Shared Channels. More information is available here: [B2B direct connect overview - Azure AD | Microsoft Docs]

When you configure B2B Direct Connect, you are specifying which external users can collaborate using Native Identities without switching tenants.

Step	Detail
1. Create an organisational relationship	a. Go to the Azure AD portal and choose External Identities under Manage, then Cross-tenant Access Settings b. Click add organisation and enter a domain name from the partner tenant and click add
2. Configure Outbound Settings	a. On the entry for the organisation, you want to manage, click “Inherited from default” under Outbound Access b. Click the B2B direct connect tab, then click Customize settings. c. On the Users and groups tab click allow access. You can optionally choose a specific group of local users who are allowed to collaborate using B2B Direct Connect d. On the External applications tab click Allow access, then under “Applies to”, click “Select external applications” and add Microsoft 365 e. Click Save
3. Configure Inbound Settings	a. Click Cross-tenant access settings on the left b. On the entry for the organisation, you want to manage, click “Inherited from default” under Inbound Access c. Click the B2B direct connect tab, then click Customize settings. d. On the Users and groups tab click allow access. You can optionally choose a specific group of external users who are allowed to collaborate using B2B Direct Connect (you must specify the object ID of the remote group) e. On the Applications tab click Customize settings then click Allow access. Under “Applies to”, click “Select applications”, click Add Microsoft applications and Microsoft 365. Click select. f. Click Save

4.5 Device Compliance Settings

If your organisation has a need to provide a higher level of confidence over the devices being used to access Microsoft 365, requiring that devices are compliant with organisational policies as part of conditional access.

Follow the guidance in the link, using the settings from the table below: Building a Conditional Access policy - Azure Active Directory | Microsoft Docs

To use device compliance in conditional access policies, your organisation must be using a Mobile Device Management solution that integrates with Azure AD such as Intune. If you are not, device compliance state will not be available for use in access control decisions.

Attribute	Value	Additional Settings
Name	Baseline Device Compliance Policy	
Assignments	Users and Groups	Include – All Users *Exclude – All guest and external users
Cloud apps or actions	All Cloud Apps	
Conditions	N/A	
Access Controls	Require device to be marked as compliant	Require all the selected controls
Enable policy	On	

Table 18 Device compliance settings

> Note: You should also exclude at least one global administrator (usually your break-glass account) from this policy to ensure that you can always log in to your tenant with at least one account. Manage emergency access admin accounts - Azure AD | Microsoft Docs

4.6 Teams

4.6.1 Teams Upgrade Mode

Unless you are running Skype for Business on-premises, switch to “TeamsOnly” upgrade mode to enable the richest chat experience (including @mentions, rich text formatting, etc).

Teams Only mode considerations - Microsoft Teams | Microsoft Docs

4.6.2 Teams Governance, Management and Lifecycle

By default, Teams sites exist until they are deleted. Retention policies (configured in **Groups – Expiration**) can set a limit, after which Teams owners are asked to renew their teams. If enabled with no further configuration, the default for this is 180 days. See Microsoft 365 group expiration policy | Microsoft Docs and Set expiration for Microsoft 365 groups - Azure Active Directory | Microsoft Docs for further details .

This helps to limit "stale" teams. Team owners are notified through the activity section 30, 15 and 1 day before expiration. Once expired, the Teams site is "soft-deleted", after which IT Admin have 30 days in which to recover the team on behalf of the user.

Please note that once this option is enabled other groups that are created via Planner, SharePoint or any other app will also be encompassed by the policy. The owners of these groups will receive notification of expiry via email.

If there is a group that is no longer used, but you wish to retain its content, see End of lifecycle options for groups, teams, and Yammer | Microsoft Docs for information about how to archive or export information from the different groups services.

Users who are Team owners need to understand the link between Teams and SharePoint. It is possible to share documents from the SharePoint site that lies behind Teams, and populates its file content, without the recipient being a member of that Team. If this is undesirable for certain Teams, then users must be educated in how to restrict that option. A very good explanation of the different scenarios available here: Managing External Guests in SharePoint vs Teams | Microsoft Docs

4.6.3 Shared Channels

Shared channels in Microsoft Teams create collaboration spaces where you can invite people who are not in the team. Only the users who are owners or members of the shared channel can access the channel. While guests (people with Azure Active Directory guest accounts in your organization.) can't be added to a shared channel, you can invite people outside your organization to participate in a shared channel by using Azure AD B2B direct connect.

Follow the guidance in the link, using the settings from the table below: Collaborate with external participants in a shared channel | Microsoft Docs

Note: Azure AD B2B direct connect needs to be enabled in order enable shared channels **B2B Direct Connect**

Teams Admin Center > Teams > Teams policies (Select the policy for which you want to enable shared channels)

Setting	Value	Impact
Create shared channels	On	Team owners can create shared channels for people within and outside the organization. Only people added to the shared channel can read and write messages.
Invite external users to shared channels	On	Owners of a shared channel can invite external users to join the channel, if Azure AD external sharing policies are configured. If the channel has been shared with an external member or team, they will continue to have access to the channel even if this control is turned off.

Table 19 Teams meeting settings

Only members of the tenants with established B2B direct connections can gain access to the shared channels.

4.6.4 Coming Soon – New Teams Application (Public Preview)

The new Microsoft Teams application for PC (currently in Public Preview) will allow people to collaborate more effectively across organizational boundaries.

It can be challenging for people to manage multiple work accounts. You cannot receive real-time notifications during calls or meetings across organisations or accounts. Switching from one organisation to another or from one account to another interrupts your workflow since it requires you to log in and out.

New Teams will enable you to collaborate more effectively across organisational boundaries by being actively signed into multiple accounts at the same time and receiving real-time notifications no matter which one is currently in use. You can seamlessly engage with people across multiple accounts and organisations without having to drop out of a call or meeting, ensuring no disruption to your workflow.

There are some limitations while the application is in Public Preview, but once New Teams is made generally available by Microsoft, it would make sense to be prepared for updating end user devices with the new application.

More information is available at the following announcement blog post:
https://techcommunity.microsoft.com/t5/microsoft-teams-blog/what-s-new-in-microsoft-teams-at-enterprise-connect-2023/ba-p/3774374

4.7 SharePoint

4.7.1 Domain Restrictions

It is possible to further restrict sharing by creating allow or deny lists that either explicitly prevent, or explicitly allow sharing for individual external organisations.

> Note: This approach is not recommended as it creates additional administrative overhead and impacts the end user collaboration experience. You should only implement allow or deny lists if deemed absolutely necessary according to your organisations risk appetite. The NCSC strongly advocate for a 'default-allow, explicit-deny' approach to authorising sharing. This approach means that a user is allowed to share access with a given recipient as long as they are not covered by a deny list.

It's important to understand the differences between a Team and the SharePoint site that underpins it. A good explanation can be found here:

Managing External Guests in SharePoint vs Teams | Microsoft Docs

If you want to control individual file sharing in SharePoint, you can set up an allow or deny list for OneDrive and SharePoint. It is also possible to restrict domains on a SharePoint site collection level for sensitive sites. Reference: Domain restrictions when sharing SharePoint & OneDrive content - SharePoint in Microsoft 365 | Microsoft Docs

If any very sensitive SharePoint sites exist, where collaboration must be further restricted, then this can be configured following this guidance: Change the sharing settings for a site - SharePoint in Microsoft 365 | Microsoft Docs

4.8 Exchange

4.8.1 Organisational Relationships for Calendar Availability

Section 4.6.2 describes how to configure organisational relationships in the Exchange Online portal. You can also use PowerShell to create organisational relationships using a published list of government organisations. A description of how to do this is below. Please note that if any calendar sharing agreements are in place already, their domains must be omitted from the command, or removed from their current sharing relationship and added to the new one. An example is shown below:

```
New-OrganizationRelationship -Name "Calendar Sharing" -DomainNames "contoso.com",
"woodgrovebank.com" -FreeBusyAccessEnabled $true -FreeBusyAccessLevel AvailabilityOnly
```

The command should contain the full published list of participating organisations.

If failures occur when running the command to create the organisation relationship, it may be that some of the organisations are already configured. You can list the current organisational relationships by running the following command:

Get-OrganizationRelationship

4.8.2 MailTips

In order to guide users in appropriate sharing behaviour, various MailTips can be configured as documented in MailTips in Exchange Online | Microsoft Docs

While there are several 'out of the box' MailTips that can be used to provide helpful information when sending certain types of mail in various scenarios, it is possible to create Custom MailTips. Custom MailTips can detect a Recipient Type, such as a specific person, group, or other defined type, and could be used to remind users when they are emailing external recipients, about the best practice of only sharing information when necessary.

4.8.3 Showing Guest Users in the Global Address List

By default, guest users are not visible in the Global Address List. It can be useful to make guest users visible in the GAL to aid collaboration and sharing. In order to show them you should follow guidance in the "Add guests to the Global Address List" section in Prevent guests from being added to a specific group | Microsoft Docs

5 Configuration Settings Checklist

The table below contains an index of the settings to be applied to your tenants. It contains links to the guidance for each setting, and a reference to the document section containing the settings to apply. Work through this list to implement the baseline configuration after you have reviewed and implemented the guidance described in section 1.4 above.

Configuration Theme	Configuration Setting	External Link to Microsoft Guidance	Specific settings section
Auditing	Advanced Auditing	Set up Advanced Audit in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs	Refer to O365 Blueprint section 4.2.1 O365 Blueprint (microsoft.com)
	Audit Retention	Manage audit log retention policies - Microsoft 365 Compliance | Microsoft Docs	Refer to O365 Blueprint section 4.2.1 O365 Blueprint (microsoft.com)
Guest Access Settings	External Collaboration Settings	Enable B2B external collaboration settings - Azure AD | Microsoft Docs	2.1.1
	Cross-tenant Access	Configure B2B collaboration cross-tenant access - Azure AD | Microsoft Docs	2.1.2
	Conditional Access Policies for Guests (including MFA and Terms of Use)	Create a secure guest sharing environment | Microsoft Docs	2.1.3
	One-time Passcode Authentication	One-time passcode authentication for B2B guest users - Azure AD | Microsoft Docs	2.1.4
	Entitlement Management Settings	Govern access for external users in Azure AD entitlement management - Azure Active Directory | Microsoft Docs	2.1.5
Device Compliance Settings	Conditional Access for Device Compliance	Building a Conditional Access policy - Azure Active Directory | Microsoft Docs	2.1.6
Organisational Policy	Anonymous Calendar Sharing	Share calendars with external users - Microsoft 365 admin | Microsoft Docs	2.1.7

Configuration Theme	Configuration Setting	External Link to Microsoft Guidance	Specific settings section
Microsoft Teams	Guest Access Settings	Manage guest access in Microsoft 365 groups - Microsoft 365 admin | Microsoft Docs Guest access in Microsoft Teams - Microsoft Teams | Microsoft Docs	2.2.1
	External Access	Manage external access (federation) - Microsoft Teams | Microsoft Docs	2.2.2
	Teams Settings	Manage settings for your organization - Microsoft Teams | Microsoft Docs	2.2.3
	Meeting Settings	Manage meeting settings - Microsoft Teams | Microsoft Docs	2.2.4
	Meeting Policies	Teams: Manage meeting policies - Microsoft Teams | Microsoft Docs	2.2.5
	Shared Channels	Collaborate with external participants in a shared channel | Microsoft Docs	4.3.3
SharePoint Online	SharePoint Policies	Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Docs	2.3.1
	Enable Azure AD B2B integration for SharePoint and OneDrive	Azure AD B2B integration for SharePoint & OneDrive - SharePoint in Microsoft 365 | Microsoft Docs	2.3.2
OneDrive	Sharing	Control notifications - OneDrive | Microsoft Docs	2.4.1
Exchange Online	Message Filtering	Configure junk email settings on Exchange Online mailboxes - Microsoft 365 | Microsoft Docs	2.5.1
	Calendar Free/Busy (Organisational Sharing Policy)	Create an organization relationship in Exchange Online | Microsoft Docs	2.5.2
	Restricting Calendar Sharing	Create a sharing policy in Exchange Online | Microsoft Docs	2.5.3