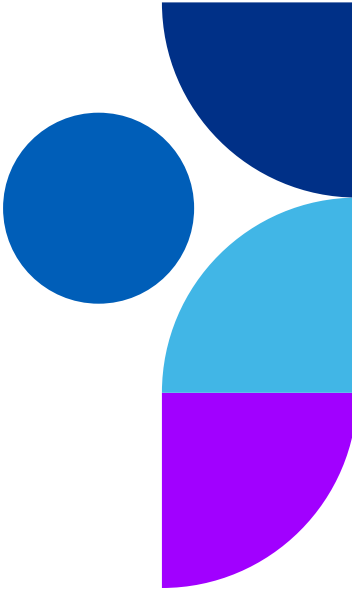
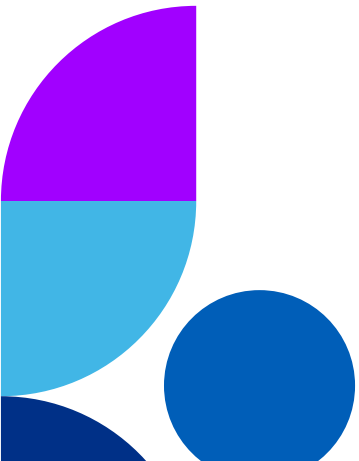




Microsoft 365 Copilot Chat Browser Management Technical Guidelines

(September 2025 – v1.0)



Contents

Microsoft 365 Copilot Chat Browser Management Technical Guidelines	3
Overview	3
Managing Browser Third Party Cookies	4
Laptop/Desktop Devices: Option 1	5
Laptop/Desktop Devices: Option 2	7
Laptop/Desktop Devices: Option 3	7
Mobile Devices: Intune Managed Devices	8
Microsoft Copilot – Browser Management Policies	9
Disable the Chat Page Context Feature in Microsoft Edge	9
Allow or Block Copilot Chat in Edge from Using Browsing Context	11
Disable Microsoft 365 Copilot Chat in Edge	13
Manage Copilot Chat Access for Personal MSA Accounts in Work Profiles	15
Manage access to Microsoft Copilot (Consumer version) at Network Level	16

Microsoft 365 Copilot Chat Browser Management Technical Guidelines

Overview

This document provides technical guidelines for managing Microsoft 365 Copilot Chat access in browsers, with a focus on Microsoft Edge. It includes instructions and best practices to help NHS organisations securely and efficiently control user access via Microsoft Intune, Group Policy Objects (GPOs) and network configurations.

This document is intended for NHS Local Administrators within NHS organisations.

Note: The information provided in the sections above is general guidance and might get obsolete over time. It's local administrators' responsibility to validate any settings/configuration.

Managing Browser Third Party Cookies

Cookies are minor data files that websites save on a computer to track users' preferences. Most browsers allow cookies by default. This includes both first-party and third-party cookies.

For Microsoft 365 Copilot to work in Word Online, Excel Online and PowerPoint Online, your organisation will be required to enable third-party cookies within the browsers. To facilitate this, action should be taken as explained below.

Action Required

As noted above, please ensure third party cookies are enabled on the corporate devices of all M365 Copilot licensed users. To facilitate this, one action should be taken for laptop/desktop devices, and one action should be taken for mobile devices:

For Laptop and Desktop devices - complete one of the following actions:

- **Option 1:** If you are using Microsoft Intune, create a Device Configuration Profile – Setting Catalog to enable third-party cookies.
- **Option 2:** If you are using Microsoft Intune, create an App Configuration Profile for Managed Apps for Microsoft Edge for Windows.
- **Option 3:** If M365 Copilot licensed users are to use a device (i.e. laptop/desktop) which is managed by a local device management solution, conduct the necessary configuration through GPO (Group Policy Objects).

For Mobile Devices – the type of device will determine which action should be taken.

- **Intune-Managed Devices:** Configure settings within Microsoft Edge
- ***Devices managed by a local device management solution:*** Please review your relevant local MDM documentation and take the necessary steps.

Laptop/Desktop Devices: Option 1

If you are using Microsoft Intune, create a Device Configuration Profile – Setting Catalog to enable third-party cookies

Windows – Edge Browser

1. Create profile: Devices → Configuration → Create → Windows 10 and later → Settings catalog.
2. Add setting: Microsoft Edge → set “Block third party cookies” and “Block third party cookies(user)” to Disabled.
3. Assign & validate: Deploy to target groups and validate.

Official documentation reference: [Deploy Microsoft Edge policy using settings catalog in Microsoft Intune](#)

Windows – Chrome Browser

1. Create profile: Devices → Configuration → Create → Windows 10 and later → Settings catalog.
2. Add setting: Google Chrome → set “Block third party cookies” and “Block third party cookies(user)” to Disabled.
3. Assign & validate: Deploy to target groups and validate.

Official documentation reference: [Manage Chrome browser with Intune Settings Catalog \(Windows\)](#)

MacOS – Edge Browser

1. Create profile: Devices → Configuration → Create → macOS → Settings catalog.
2. Add setting: Microsoft Edge Apple → set “Block third party cookies” to Disabled
3. Assign & validate: Deploy to target groups and validate.

Official documentation reference: [Deploy Microsoft Edge policy using settings catalog in Microsoft Intune](#)

MacOS – Chrome Browser

1. Intune admin center → Devices → Configuration → macOS → Create → Templates → Preference Template.
2. Configuration settings: Import the .plist file with required settings to block third party cookies.

```
<key>BlockThirdPartyCookies</key>  
<true/>
```

3. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Enrol browsers with Microsoft Intune \(macOS\)](#)

[Chrome Enterprise policy list and management](#)

[Allow or restrict third-party cookies - Chrome Enterprise](#)

MacOS – Safari

Intune's macOS device restrictions profile lets you control some Safari features (e.g., block AutoFill, disable camera), but there is no setting in Intune's Settings catalog to toggle "Allow third-party cookies". Your organisation has the option to use a Custom Device Configuration template to assign settings that are not built into Intune yet. Please refer to this link: [Add custom settings to macOS devices in Microsoft Intune](#)

Note: Safari blocks third-party cookies by default for privacy reasons. Users can manually allow them by:

1. Open Safari → Settings (or Preferences) → Privacy.
2. Uncheck "Prevent cross site tracking" and uncheck "Block all cookies" (if enabled).
3. Restart Safari for changes to apply.

Official documentation references:

[Manage cookies and website data using Safari](#)

[Add custom settings to macOS devices in Microsoft Intune](#)

Laptop/Desktop Devices: Option 2

If you are using Microsoft Intune, create an App Configuration Profile for Managed Apps for Microsoft Edge for Windows.

1. Sign in to the Microsoft Intune admin center.
2. Choose, Apps > Windows > Configuration > Create.
3. Target: *All Microsoft Apps*.
4. Add settings > Microsoft Edge/ Uncategorized > Set “*Block Third Party Cookies*” to Disabled.
5. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Configuration policies for Intune App SDK managed apps](#)

[Microsoft Edge Browser Policy Documentation](#)

Laptop/Desktop Devices: Option 3

If M365 Copilot licensed users are to use a device (i.e. laptop/desktop) which is managed by a local device management solution, conduct the necessary configuration through GPO (Group Policy Objects).

Please ensure Windows devices have the following settings enabled:

Administrative Template	Settings	Value
Microsoft Edge	Block third party cookies	Disabled
Google Chrome	Block third party cookies	Disabled

To setup Google Chrome on Domain-joined devices, please refer to [setting Chrome Browser policies on Managed PCs](#).

Note: The information provided in the sections above is general guidance and might get obsolete over time. It's local administrators' responsibility to validate any settings/configuration.

Mobile Devices: Intune Managed Devices

Microsoft Edge is the only approved browser for accessing corporate data using nhs.net accounts on Microsoft Apps. This down to the configuration of app protection policy. For instance, if you attempted to visit office.com using the Chrome or Safari browser, you will be prompted to open or download the Microsoft Edge App on your mobile device.

For Intune-managed devices, the following steps should be taken, dependent on the device type:

iOS/iPadOS – Microsoft Edge

Edge for iOS does not support controlling cookies. This is by design. For further details, please refer to [Control Cookie Mode](#).

Android – Microsoft Edge

1. Sign in to the Microsoft Intune admin center.
2. Choose, Apps > Configuration > Create > Managed apps.
3. Click “+ Select public apps”. In the search box, enter Microsoft Edge.
4. Select Microsoft Edge (Android).
5. Settings > General configuration settings.
6. Add the required configuration information.
 - **Name:** com.microsoft.intune.mam.managedbrowser.cookieControlsMode
 - **Value:** 0
7. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Control Cookie Mode](#)

[App configuration policies for Microsoft Intune](#)

[Add app configuration policies for managed Android Enterprise devices - Microsoft Intune](#)

Note: Microsoft doesn't recommend managing third-party cookies for specific domains because the URLs required for Microsoft 365 Copilot to function with Microsoft 365 apps may change over time. This introduces ongoing maintenance and management overhead to track deprecated or updated URLs.

However, if your organization has a strict requirement to allow third-party cookies for specific URLs, ensure that you only enable them for the URLs listed in the official Microsoft documentation here:

[Microsoft-365-unified-domains](#)

[Microsoft-365-common-and-office-online](#)

Note: The information provided in the sections above is general guidance and might get obsolete over time. It's local administrators' responsibility to validate any settings/configuration.

Microsoft Copilot – Browser Management Policies

Disable the Chat Page Context Feature in Microsoft Edge

This policy controls whether Microsoft 365 Copilot in the Microsoft Edge sidepane can access Microsoft Edge page content. This includes page summarization and similar contextual queries sent to Copilot. Refer official documentation [Microsoft Edge Browser Policy Documentation EdgeEntraCopilotPageContext | Microsoft Learn](#).

Local admins can implement this policy:

Using GPO (Windows)

1. Open Group Policy Editor (gpedit.msc).
2. Navigate to: Computer Configuration > Administrative Templates > Microsoft Edge.
3. Find: Control Copilot access to Microsoft Edge page content for Entra account user profiles.
4. Set to Disabled.
5. Run gpupdate /force

Official documentation reference:

[Microsoft Edge Browser Policy Documentation EdgeEntraCopilotPageContext](#)

[Configure Microsoft Edge for Windows with policy settings](#)

Using Registry (Windows)

- Registry Path: [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
- Key: EdgeEntraCopilotPageContext
- Value type: dword
- Value: 00000000

Official documentation reference:

[Microsoft Edge Browser Policy Documentation EdgeEntraCopilotPageContext](#)

Using Intune (Windows)

1. Go to Intune Admin Center → Devices → Manage Devices → Configuration → New policy.
2. Create profile: Platform: Windows 10 and later / macOS.
3. Settings: Microsoft Edge → Select “*Control Copilot access to Microsoft Edge page content for Entra account user profiles when using Copilot in the Microsoft Edge sidepane*”.
4. Set to Disabled.
5. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation EdgeEntraCopilotPageContext](#)

[Deploy Microsoft Edge policy using settings catalog in Microsoft Intune](#)

Using Intune (macOS)

1. In Intune, go to Devices > macOS > Configuration > Create policy > Select Profile type “Templates” > Preference file >
2. Create a .plist file with the required domain and key-value pairs. Example:

```
<key> EdgeEntraCopilotPageContext</key>  
<false/>
```

3. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation EdgeEntraCopilotPageContext](#)

[Add preference file settings to macOS devices in Microsoft Intune](#)

Note: The information provided in the sections above is general guidance and may become obsolete over time. It is local administrators’ responsibility to validate any settings/configuration.

Allow or Block Copilot Chat in Edge from Using Browsing Context

This policy controls access to page contents for Copilot in the Microsoft Edge sidebar for MSA account profile. Refer Official documentation [Microsoft Edge Browser Policy Documentation CopilotPageContext | Microsoft Learn](#).

Local admins can implement this policy:

Using GPO (Windows)

1. Navigate to Computer Configuration > Administrative Templates > Microsoft Edge.
2. Locate the policy.
3. Set to Disabled.

Official documentation reference:

[Microsoft Edge Browser Policy Documentation CopilotPageContext](#)

Using Registry (Windows)

- Registry Path: [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
- Key: CopilotPageContext
- Value: dword:00000000

Official documentation reference:

[Microsoft Edge Browser Policy Documentation CopilotPageContext](#)

Using Intune (Windows)

1. Go to Intune Admin Center → Devices → Manage Devices → Configuration → New policy.
2. Create profile: Platform: Windows 10 and later / macOS > Setting catalog.
3. Settings: Microsoft Edge → Select “Control Copilot access to page context for Microsoft Entra ID profiles”.
4. Set to Disabled.
5. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation CopilotPageContext](#)

[Deploy Microsoft Edge policy using settings catalog in Microsoft Intune](#)

Using Intune (macOS)

1. In Intune, go to Devices > macOS > Configuration > Create policy > Select Profile type “Templates” > Preference file >
2. Create a .plist file with the required domain and key-value pairs. Example:

```
<key> CopilotPageContext</key>  
<false/>
```

3. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation CopilotPageContext](#)

[Add preference file settings to macOS devices in Microsoft Intune](#)

Using Intune (iOS/Android)

Follow the steps as explained here [Manage Microsoft Edge on iOS and Android with Intune](#) for app configurations and set following setting key:

- Key: com.microsoft.intune.mam.managedbrowser.ChatPageContext
- Value: false

Note: The information provided in the sections above is general guidance and may become obsolete over time. It is local administrators' responsibility to validate any settings/configuration.

Disable Microsoft 365 Copilot Chat in Edge

This removes the Copilot Chat icon and disables its functionality. It is a new policy for edge version 139 & above. Local admins can implement this policy:

Using GPO and Registry

Use policy *HubsSidebarEnabled* as explained here [Microsoft Edge Browser Policy Documentation HubsSidebarEnabled](#).

Note: The policy [HubsSidebarEnabled](#) will be replaced by the policy [Microsoft365CopilotChatIconEnabled](#) soon

Using Intune (Windows)

1. Go to Intune Admin Center → Devices → Manage Devices → Configuration → New policy.
2. Create profile: Platform: Windows 10 and later / macOS > Setting catalog.
3. Settings: Microsoft Edge → Select “Show Hubs Sidebar”.
4. Set to Disabled.
5. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation HubsSidebarEnabled](#)

[Microsoft Edge Browser Policy Documentation Microsoft365CopilotChatIconEnabled](#)

[Deploy Microsoft Edge policy using settings catalog in Microsoft Intune](#)

Using Intune (macOS)

1. In Intune, go to Devices > macOS > Configuration > Create policy > Select Profile type “Templates” > Preference file >
2. Create a .plist file with the required domain and key-value pairs. Example:

```
<key> HubsSidebarEnabled</key>
<false/>
```

3. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Microsoft Edge Browser Policy Documentation HubsSidebarEnabled](#)

[Microsoft Edge Browser Policy Documentation Microsoft365CopilotChatIconEnabled](#)

[Add preference file settings to macOS devices in Microsoft Intune](#)

Intune for Mobile (iOS/Android)

1. Sign in to the Microsoft Intune admin center.
2. Choose, Apps > Configuration > Create > Managed apps > Choose iOS/iPadOS.
3. Targeted app: Microsoft Edge.
4. Public apps > Select public apps > Targeted apps blade > select "Microsoft Edge" for iOS and Android Set:
5. Settings > Edge configuration settings > Set:
 - Configuration key: com.microsoft.intune.mam.managedbrowser.Chat
 - Configuration value: false
6. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Manage Microsoft Edge on iOS and Android with Intune - Policy](#)

[Manage Microsoft Edge on iOS and Android with Intune - Copilot](#)

Note: The information provided in the sections above is general guidance and may become obsolete over time. It is local administrators' responsibility to validate any settings/configuration.

Manage Copilot Chat Access for Personal MSA Accounts in Work Profiles

It restricts Copilot usage when users are signed in with personal Bing accounts in Edge work profile. Local administrators can implement this:

Using Intune (Windows)

1. Go to Intune Admin Center → Devices → Configuration → New Policy.
2. Platform: Windows 10 and later
Profile type: Settings catalog
3. Settings:
Microsoft Edge → Set “Restrict which accounts can be used to sign in to Microsoft Edge” to Disabled
4. Assign & validate: Deploy to target groups and validate.

Official documentation reference: [Microsoft Edge Browser Policy Documentation RestrictSigninToPattern](#)

Using Intune (MacOS)

For Mac, you need to create preference key name “*RestrictSigninToPattern*”

1. In Intune, go to Devices > macOS > Configuration > Create policy > Select Profile type “Templates” > Preference file >
2. Create a .plist file with the required domain and key-value pairs. Example:

```
<key> RestrictSigninToPattern </key>  
<string>.*@contoso.com</string>
```

3. Assign & validate: Deploy to target groups and validate.

Official documentation references:

[Add preference file settings to macOS devices in Microsoft Intune](#)

[Microsoft Edge Browser Policy Documentation RestrictSigninToPattern](#)

Mobile Devices

This specific policy is not natively supported in the same way as desktop platforms. Although the policy itself is not directly applicable, you can enforce equivalent restrictions using Microsoft Intune and App Protection Policies. The below reference document might be useful to achieve this:

[Manage Microsoft Edge on iOS and Android with Intune](#)

Note: The information provided in the sections above is general guidance and may become obsolete over time. It is local administrators' responsibility to validate any settings/configuration.

Manage access to Microsoft Copilot (Consumer version) at Network Level

To restrict access to Microsoft Copilot (consumer) at network level, set your corporate proxy to block endpoints/URLs such as **bing.com/chat** and **copilot.microsoft.com**. As it will block Copilot (consumer) at network layer, no browser/app will be able to access it. Find more details [Manage Microsoft 365 Copilot Chat](#)

Note: Microsoft does not officially recommend this approach, and it may affect users with licensed access. It should be noted that these URLs may change over time..

Last reviewed date	1 October 2025
---------------------------	----------------