Microsoft

Strategy

Microsoft 365 Collaboration Blueprint for UK Government

Prepared for UK Government

15th June 2022

Version 1.0

Prepared by

Microsoft Industry Solutions

1 Intended Audience

This document is intended for UK government stakeholders with a responsibility, interest or remit related to the configuration of Microsoft 365 tenants to support a standardised approach to collaboration across and within government organisations. Decision-makers with responsibility for the implementation of Microsoft cloud services may refer to this document for further information supporting the documented recommended configuration.

Technology professionals in government organisations may find this document useful in providing further explanation and justification of specific configuration areas, particularly where there is a conflict with existing configurations or a query about the rationale behind a particular configuration area. Audiences can expect to use this document to inform technology roadmap discussions and support individual organisational strategies related to collaboration.

This document is not intended to be used as a guide to actual configuration items and settings, this level of detail can instead be found in the '*Microsoft 365 Collaboration Blueprint for UK Government: Technical Guide*'. Both documents have been produced by Microsoft and the Central Digital & Data Office (CDDO) in consultation with officials from a variety of government organisations.

2 Executive Summary

The Central Digital & Data Office aims to deliver a brilliant employee experience enabled through accelerating technical interoperability, allowing seamless working in a connected Civil Service that delivers better public outcomes. One objective is to create a set of technical standards for the secure configuration of Microsoft 365 that enables a consistent collaboration experience across HMG organisational boundaries and therefore across Microsoft 365 tenants. This is a joint engagement between CDDO and Microsoft Industry Solutions Delivery.

The programme aims to publish documentation for consumption by a government audience that includes government departments, agencies and public bodies, and their respective users of Microsoft technology. The documentation includes:

- A **Technical Guide** detailing the necessary settings and options required to deliver a consistent collaboration experience across tenants.
- A **Strategy** (this document) outlining suitable approaches to collaboration, security, and identity, providing further detail behind the recommended configuration items.

The programme identified real end user needs and challenges that could be addressed using Microsoft 365, established using a series of remote workshops to engage with a broad collection of end users. This informed a set of user stories, which then went on to be prioritised in order of value to both the individual and the organisation. Addressed in order of priority, each user story drove a particular technical item or 'setting' in the Technical Guide.

The Technical Guide was tested and iterated in the first half of 2022 by a group of five central government departments.

A major output from our research was a clear call from users for *open collaboration*. Based on input from NCSC and other security associates, the programme recommends an open approach to external collaboration, empowering users to decide who they can share information with, rather than using a restrictive 'Allow List' approach.

2.1 Building Upon Existing Guidance

The National Cyber Security Centre (NCSC) has been a key collaborator on this cross-government collaboration guidance, which builds upon the secure foundation documented in the *Office 365 UK Blueprint - Secure Configuration Alignment,* the adoption of which is essential to enabling better external collaboration.

> *By following the* Secure Configuration Alignment *and applying the cross-government collaboration guidance on top, it is the NCSC's view that Microsoft 365 can be appropriately configured to protect organisation data against the threat profile for the OFFICIAL classification when collaborating and sharing information between government departments. The NCSC expects that guidance related to collaboration and security is implemented in its entirety to avoid gaps and weaknesses leading to increased risk of a data breach.*
>
> *The NCSC believes that modern cross-organisation collaboration services that share access to information via its originating system will be more secure than traditional methods such as sending copies as email attachments to external organisations. By using modern collaboration practices, such as those described in this guidance, organisations have greater auditing and visibility of how their data is being handled and more options for owning who and where their information is handled.*
>
> *To get the functional and security benefits of modern collaboration services, organisations need to allow them to be used to collaborate with the same people and organisations that they currently do. For example, applying equivalent policies to those that are already applied to outgoing email attachments. The NCSC expect that this will be a default-allow approach for organisations handling OFFICIAL information (including that with the OFFICIAL–SENSITIVE caveat).*

3 Principles

As identified during multiple workshops with end users in late 2021, the overall user experience when collaborating between government organisations was inconsistent and could be more secure. The need for civil servants to work together, or collaborate, is increasingly important for providing an efficient public service. People and information are not always easily accessible when they are in separate organisations, buildings, or technology environments; this creates frustration for those who need to collaborate with colleagues from other organisations to do their work, often lengthening the time it takes them to complete tasks.

Technology can be part of the problem, for example when two or more organisations use technology in different ways due to differing strategies or principles, or due to varying degrees of adoption of new features and functionality. This can provide an unintuitive user experience. Looking at the end user experience when specifically using Microsoft collaboration technology to work together across government organisations, there were several areas identified for improvement.

To improve consistency and security, CDDO determined that there would be a centralised baseline configuration for core collaboration elements in government Microsoft 365 tenants that should be adopted by all organisations. We recognised that each organisation may have specific requirements for differing configurations, and so the Technical Guide is intended to be used as a baseline upon which each organisation can build. This will provide as consistent an experience as possible, within the limits of the organisation.

The improvements that were identified have been incorporated into the recommended configuration. Each of them has a validated reason for forming part of the configuration by either improving consistency or enhancing security.

4 Collaboration

Increasingly in our modern world, there is a need to collaborate across boundaries with people that work for other organisations, in different locations, using different devices, at different times. Across government there is evidence of successful 'external collaboration,' but the user experience is inconsistent between organisations.

An open approach to collaboration is recommended, where users can potentially invite people from any other organisations to collaborate. As a principle, the Collaboration Blueprint does not advocate use of an Allow List, which can be difficult to maintain and could become restrictive. It also requires that organisations do not use 'Tenant Restrictions' or other means to prevent users accessing 'other' Microsoft tenants, which have been used occasionally in the past.

Organisations can still use a Deny List to ensure that some key domains are not allowed as guests if required, e.g., live.com. Certain security stances may require a deviation from this approach, but that should be by exception rather than default.

To enhance cross-government collaboration in alignment with the principles, specifically in relation to Microsoft technologies, there are several configuration elements contained within the Technical Guide that require implementation. These recommended configuration elements should improve an organisation's security posture at the same time as bettering the end user experience when working across organisational boundaries. The Technical Guide builds upon the previously published Office 365 UK Blueprint - Secure Configuration Alignment guidance, it does not replace it. Organisations should ensure that they have adopted the most recently published version of this too.

Several specific scenarios were identified during end user research workshops that represented an opportunity to enhance the user experience when collaborating across government organisations. For example, sharing access to documents between government organisations so that co-authoring can take place, or having external guests join an ongoing conversation in Teams, are both areas where consistency can be improved.

Focusing on Microsoft technology, which is widely in use across government organisations, we often use the following 'core' tools within Microsoft 365 to conduct the work:

- Microsoft Exchange Online – for calendar and email
- Microsoft SharePoint Online – for document libraries and supporting the use of Teams
- Microsoft Teams – for IM or chat, sharing, meetings, and increasingly more types of collaboration
- Microsoft Office – the desktop and web applications that end users interact with when using the products, such as Outlook.

4.1 Sharing

One of the main types of collaboration is the sharing of information. This has traditionally been done by people sending an email to the other person with the information, or document, as an email attachment. It is widely recognised that this type of sharing presents a risk to the information due to there being multiple copies stored in multiple locations or mailboxes. It also does not allow for real time co-authoring or editing and can slow down collaboration.

A more efficient and controlled way to share information is by 'sharing' a document using Microsoft 365 whereby a link to access the document is sent instead of releasing a copy of it by attaching the document to an email. This is in widespread use inside organisations that have adopted Microsoft 365, but external sharing in government is less common due to concerns about the safety of the information or fears of breaching a policy. There are different scenarios where sharing access to a document is appropriate and simple, while remaining secure. Some scenarios involve a more structured approach where users are invited to collaborate on a persistent basis, within an established team, and some scenarios will arise on a more ad-hoc basis.

When files are shared with an individual in another organisation which has its own Microsoft 365 tenant, an invitation is sent that can only be accepted by that individual, since the access is tied to the identity of that person. As part of the invitation process a guest object is automatically created for new users in the inviting tenant removing the dependency on IT to manage this process. Azure AD Business-To-Business (B2B) integration with SharePoint and OneDrive is the configuration element detailed in the Technical Guide which makes this possible.

Azure AD B2B integration is also used when adding an individual in another organisation to a Microsoft Teams site. A new guest object is created, unless the user already has a guest object in Azure AD

Structured Sharing

When setting up a collaboration space or 'site' within Microsoft 365, using Microsoft Teams or SharePoint for example, site owners often know in advance with whom they intend to share documents and information outside of their organisation. By adding external guests to Teams a guest object is created in Azure AD enabling these users to benefit from features in Microsoft Teams such as being able to tag individuals by name and linking a document that resides in a Team alongside a discussion, as well as simply sharing a link to a document ad-hoc so users know which document to work on.

Ad-hoc Sharing

Individual files can be shared with others quickly by selecting the file from within SharePoint, OneDrive, or Microsoft Teams, allowing only that document to be shared, access to other items

in the Site or Team is not granted. In this scenario a link is sent and a One-Time Password is used to securely onboard the user if they do not already have a guest object in Azure AD.

4.2 Co-Authoring

A benefit of sharing a document, rather than attaching it to an email, is that it remains in one place. This can reduce the amount of uncontrolled data and multiple versions that exist. Another advantage is that it allows end users to collaborate in real time within the same document. This 'co-authoring' experience is one that can save time and provides contextual awareness for multiple contributors, reviewers and authors when working on the same document. This can take place in a web browser or in the Office desktop applications (such as Word or Excel).

4.3 Email & Calendars

Whilst email remains a useful communication tool, its use to share attachments can limit collaboration as it does not allow co-authoring and can increase the risk of data leakage. Business Email Compromise also risks information being stolen by way of attachments being accessed without a means to revoke access when a user becomes aware of the incident.

Email should ideally be limited to scenarios that do not require instant response or it should be used for sending links to shared items.

Sharing calendars across organisational boundaries allows for more efficient scheduling of meetings and reduces the need to go back and forth to establish the availability of attendees.

4.3.1 Message Filtering

To emphasize the importance of emails containing sharing links, users should ensure that their Junk Mail settings are not configured to block emails from specific senders in government, or from system email addresses such as those used by the Microsoft 365 service. User research conducted to inform the Collaboration Blueprint highlighted concerns that such emails do not always arrive at people's inboxes. Users should be encouraged to check junk mail folders periodically.

4.3.2 Calendar Availability Sharing

To facilitate a more consistent and efficient experience when scheduling meetings across government organisations, organisations should allow calendar availability-sharing with other government organisations. It is possible to share full details of meetings in the calendar, but for privacy purposes the configuration recommends that just the 'free/busy' information is shared.

This change can enable swifter event coordination for users who need to meet with other government colleagues.

In certain circumstances where an organisation has individuals who wish to restrict the sharing of availability information, this can be achieved using per-user configuration in the Outlook client.

4.4 Microsoft Teams

Many organisations across government have adopted Microsoft Teams as a communication and collaboration tool, with core functionality such as chat or meetings now familiar to many. Within government organisations there are people using many of the features and functionality of Microsoft Teams to collaborate inside their organisation. To standardise this across organisations, there are several settings outlined in the Technical Guide.

5 Guest & External Access

Allowing Guests at an Organisation level and at a Team level is important for enabling external users to collaborate. This means that Team owners can invite external users from other organisations to join their team using the invitee's email address. Guidance from CDDO and The National Archives suggests that, subject to organisational information management policy, the 'hosting' Team owner remains responsible for the data within the team and usually no additional sharing agreement is required using this principle. 'Tenant Restrictions' or other means to prevent users accessing 'other' Microsoft tenants, which have been used occasionally in the past, should not be used as this will prevent cross-tenant collaboration on the whole and prevent ad-hoc sharing with any organisations that are not already allow listed in Tenant Restrictions.

5.1.1 Meeting Policies & Settings

Participants and guests should be able to enjoy the same rich experience within Teams meetings as hosts or participants from the source tenant. External participants can get a different Teams meeting experience than in their own organisation, which can lead to frustration and stifle collaboration.

The Technical Guide outlines settings which provide a balance between appropriate and creative. For example, allowing Gif's that are only safe for work and disallowing memes ensures that light-hearted collaboration can take place at the same time as remaining suitable for work. Other settings such as the Immersive Reader should be turned on to provide an improved accessibility stance in meetings which supports inclusivity.

File Sharing settings should be configured to disallow the use of consumer or third-party services such as Dropbox and Google Drive (unless organisational policies allow otherwise), to ensure that files are stored within the controlled environment of Microsoft 365, where the correct policies and governance can apply.

5.2 SharePoint Online & OneDrive

To make best use of modern sharing techniques such as sending links instead of attachments, users should be encouraged to store documents and files within SharePoint Online or OneDrive. When files are stored within Microsoft Teams, this uses SharePoint Online as a repository for Channel content and uses OneDrive for Chat files. Once the relevant settings and policies are applied to SharePoint Online and OneDrive, users will be able to easily share documents from here with guests and be able to set the appropriate permissions.

5.2.1 Document Governance

When storing documents in SharePoint Online and OneDrive, advice from CDDO and The National Archives is that the responsibility for the data remains with the organisation hosting the data in the source tenant. Organisations should continue to adhere to existing data governance, compliance, and information architecture best practices that are in place. Providing access to documents and data stored within a Microsoft 365 tenant should be in line with government policy, paying particular attention to document classification and handling instructions.

5.2.2 Sharing Policies & Settings

The Technical Guide recommends that open external sharing is enabled. This is based on a fundamental assumption that organisations have already implemented appropriate sharing and governance policies to guide end users when sharing information outside of the organisation. Given the emphasis on these policies it would be prudent for policymakers to review the availability and awareness of such guidance. Providing the capability to share with external organisations does not override sharing policies and end users should be encouraged to maintain a good level of awareness for the rules surrounding access to data by others.

5.3 Collaboration Roadmap

At the time of writing, several emerging features and functionality related to cross-government collaboration are not generally available but remain in public preview. As these features approach their respective release dates, plans should be made for adoption and integration.

5.3.1 Teams Connect (Public Preview)

Teams Connect removes the need to switch tenants when collaborating in a Shared Channel. Currently when collaborating across tenants, Teams requires users to switch tenants which takes time and can cause frustration. Switching tenants is also perceived as a barrier to effective collaboration.

Microsoft Teams Connect enables users to share channels in Microsoft Teams across multiple organisations. With this new capability, people can collaborate in the same digital environment with people from outside their organisation without the need to switch tenants – leveraging all the deep collaboration capabilities that only Teams brings together.

When creating a new shared channel, users will be able to invite both individuals or entire teams, assuming they have an Azure AD identity, from as many organisations as they need, while allowing your organisation to control how users access data and information.

6 Identity and Security

The secure configuration for Office 365 was updated in April 2021 for UK Public Sector customers and should be used as the baseline upon which cross-government collaboration builds. This will ensure that organisations align with the recommended security settings for wider Office 365 services.

Adherence to the settings described in the Technical Guide will reduce the risk of external collaboration resulting in information disclosure or other information breaches.

User identity is the essential foundation for the security of cross-government collaboration in Microsoft 365. It is critical to establish who the user is as it forms the foundation of trust for all subsequent interactions. Once we successfully validate the user, we can explicitly verify every element of their access.

Identity is defined as the 'control plane for IT security', and authentication is an organisation's access guard to the cloud. Organisations need an identity control plane that strengthens their security and keeps their cloud applications safe from intruders.

The recommended model for collaboration outlined in the Technical Guide moves the preferred method of sharing documents from email attachments to sharing directly from the application where the files are stored, i.e. OneDrive, SharePoint Online and Microsoft Teams. Access to collaboration spaces and documents is based on the identity presented. This increases security by:

- providing more control over how documents are shared as they never need to leave the originating organisation.
- protecting documents using Microsoft Purview Information Protection if external users request to download the document locally.
- providing visibility of whom documents are shared with, a feature which is not available when shared by email as attachments.

With the recommended approach to external collaboration, external identities need to be recognised in your organisation's Azure AD. Azure AD business-to-business (B2B) collaboration lets you invite guest users to collaborate with your organisation. The guest user authenticates within their home directory whilst allowing your organisation to assign guest users to Groups or Microsoft Teams.

The advantages of using Azure AD B2B to provision and manage Guest users include:

- The partner uses their own identities, (including Microsoft, Google and Facebook credentials) governed by their identity management solution; manual account creation in Azure AD is not necessary.
- You do not need to manage external accounts or passwords in your organisation, or to sync accounts or manage account lifecycles for guest users.
- Access to SharePoint and OneDrive sharing by people invited from outside your organisation are subject to the same Azure AD access policies (e.g. multi-factor authentication), simplifying the administration experience.

Please refer to the Invitation Redemption Flow for more detail on the logic used by Azure AD when an external user redeems their invitation request.

6.1 Approach to external organisations

Microsoft provides several control points where an organisation can restrict the organisations with which they can collaborate externally. Restricting who users can collaborate with increases the operational overhead needed to support maintaining the list of allowed organisations. In addition, the 'Allow List' approach will prevent ad-hoc collaboration with any external organisation or individuals not included in the Allow List, which can cause delays and frustration and can lead to users finding alternative methods to share information which may reduce security.

Based on user feedback and advice from NCSC, CDDO and Government Security Group, the recommended approach is to allow external collaboration between any organisation by default. As with the traditional approach to sharing by email, this relies on users accepting personal responsibility and exercising good judgement. However, the modern collaboration model brings greater detection and response capability over traditional email attachments by employing monitoring and auditing where the documents have been shared. This aligns with Government Security Policy Framework.

> **Important**
>
> Additional control can be provided with this approach by using a 'Deny List' that includes the namespaces for organisations or top-level DNS namespaces which are deemed to pose active threats.

The use of a restrictive Allow List precludes ad-hoc collaboration with organisations and individuals who are not included in the list of allowed domains. If an organisation's threat profile

or risk appetite is such that they are not able to use the recommended open approach to collaboration an Allow List approach can be used.

In this case, ensure that there is a clearly defined and articulated process to allow users to request that an organisation is added to the Allow List.

6.2 Multi-factor authentication

Protecting accounts with Multi-Factor Authentication (MFA) reduces the chances of an account being compromised by providing protection against common cyber-attacks or in case of a data breach. It is especially important to require multi-factor authentication for guests even if they are from another Government organisation, partner, or supplier. If a guest's username and password is stolen, requiring a second factor of authentication reduces the chances of unknown parties gaining access to information that has been shared with them.

The NCSC's guidance on multi-factor authentication for online services states:

> *"All users, including administrators, should use multi-factor authentication when using Cloud and Internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data."*

The recommended approach for enforcing MFA for all guest users is using Conditional Access, as defined in the Technical Guide.

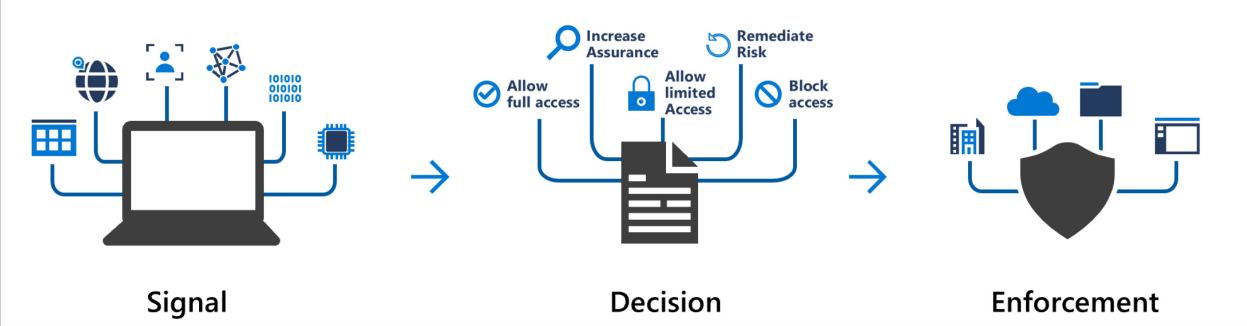
6.3 Enhanced Identity & Access Management

In a minority of circumstances, some government organisations may wish to enhance the security posture of Identity & Access Management. For instance, organisations that operate in a more sensitive and restricted environment might wish to apply another layer of security to the recommended configuration. Doing so introduces an additional level of technical complexity and impacts the user experience, which organisations should consider carefully.

6.3.1 Conditional Access using Session Control

If an organisation determines that their threat profile demands a more risk-averse approach, Conditional Access Session Control can be employed. This forces the external user to use web applications where additional controls can be enforced, e.g., block download, cut, copy, and print of sensitive documents on, for example, unmanaged / Bring Your Own Device (BYOD) devices or Guest devices from another organisation whose health state cannot be determined so have to be considered as unmanaged / BYOD so session control should be enforced using Microsoft Defender for Cloud Apps.

Conditional Access is the tool used by Azure Active Directory to bring intelligent digital 'signals' together, to make decisions, and enforce organisational policies. Conditional Access is at the heart of Microsoft's Zero Trust security model and the identity driven control plane that provides the authorisation to cloud applications like Microsoft Teams and SharePoint Online.



The image **Error! Reference source not found.** describes Conditional Access components with Zero Trust model alignment. Details of the signals that are used by conditional access are described in more detail here and Conditions in Conditional Access policy - Azure Active Directory | Microsoft Docs

6.3.2 Entitlement Management

If an organisation determines that they require an enhanced governance position, then Azure AD Entitlement Management can be employed to address this need.

Entitlement Management is an Azure AD identity governance capability that enables organisations to manage Identity & Access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration of this access if necessary. It also automates the creating and deprovisioning of guest users in Azure AD. Entitlement Management requires a formal connection between organisations to be configured.

Entitlement Management uses the concept of an '*access package*', a grouping of resources that a user needs access to, e.g. Microsoft Teams or SharePoint Online sites. Access packages are used to govern access for both internal and external users.

Access packages enable business users, instead of IT admins, to manage access for external collaborators, reducing the overhead on IT admin teams. They can define policies with rules for which users can request, who must approve their access (this is not mandatory), and crucially when their access expires.

Entitlement Management should be considered for organisations who are looking to delegate external collaboration to the business or whose threat profile indicates that the enhanced governance capabilities provided by Entitlement Management will help reduce the risk associated with external collaboration.

6.4 Identity and Security Roadmap

As the following features approach their respective release dates, plans should be made for adoption and integration. At the time of publishing, these features are not yet generally available.

6.4.1 Cross Tenant Access (Public Preview)

Whilst MFA provides protection and verification for guest user identities, it does not provide any information on the state or health of the guest device being used. As a result, access controls cannot safely assume the security condition of the device as part of the external collaboration pattern. There is currently no method of establishing whether the device that is used by a given guest to access data is healthy or managed. Therefore, in theory, they should be treated in a similar manner to Bring Your Own Devices (BYOD).

The UK Blueprint for BYOD guidance that Microsoft published in June 2020 state that users should only be allowed to have access to Office 365 applications in a Web Browser from their personal PC or Mac devices and are prevented from downloading files or attachments. This is to ensure corporate data is not persistently stored in an unmanaged location/environment.

The experience for external users is critical to the success of collaboration. For cross-government collaboration, the web browser-only user experience would be suboptimal and could lead to poor adoption and potential use of shadow IT services. These services are unlikely to align with the organisation's security or data governance policies and therefore constitute an unknown risk.

Microsoft has released Cross Tenant Access feature in Azure AD that will enhance the access control options available for Guest Devices that are managed by partner organisation. These are devices that are corporately managed by a partner organisation and are joined or registered in their Azure AD. Cross Tenant Access policies allow device health attestation from partnered organisations to be presented during the authentication request to access your information. If an external collaboration partner organisation has not enrolled into Cross Tenant Access then the recommendation is to use Office Web Apps only in alignment with and the UK Blueprint for BYOD guidance.

Until the use of Cross Tenant Access Policies becomes prevalent across government, organisations should conduct their own risk analysis of restricting collaboration to only in web apps or enabling use of desktop apps.

6.4.2 Azure AD B2B Direct Connect (Public Preview)

Azure AD B2B direct connect is a feature of External Identities in Azure AD that lets you set up a mutual trust relationship with another Azure AD organisation for seamless collaboration. This feature currently works with Microsoft Teams shared channels, refer to Section 5.3.1 above for more detail.

With B2B direct connect, users from both organisations can work together using their respective organisation's credentials and a shared channel in Teams, without having to be added to each other's organisations as guest accounts.

Both the resource organisation and the external organisation need to mutually enable B2B direct connect in their cross-tenant access settings. When the trust is established, the B2B direct connect user has single sign-on access to resources outside their organisation using credentials from their home Azure AD organisation.

> **Important**
>
> Both Cross Tenant Access and B2B Direct Connect are required to allow Teams Connect to be implemented.

7 Conclusion

The Collaboration Blueprint for UK Government was created to promote a consistent user experience for people collaborating across government when using Microsoft 365. This consistency can only be realised if as many organisations as possible, across government, implement the guidance. If there are potential barriers to this in your organisation, we recommend you discuss this via the usual Microsoft account management channels, where advice and guidance can be provided.

It is important to remember that the Collaboration Blueprint should be used to build upon the guidance in the *Office 365 UK Blueprint - Secure Configuration Alignment* as recommended by the NCSC. Together, this represents a configuration that is both consistent and secure for each organisation.

The Collaboration Blueprint is intended to be updated over time. The inclusion of sections for Roadmap features was intended to give the audience some background on useful functionality that could become part of the standard guidance in future updates as new capabilities are developed that improve the collaboration experience.