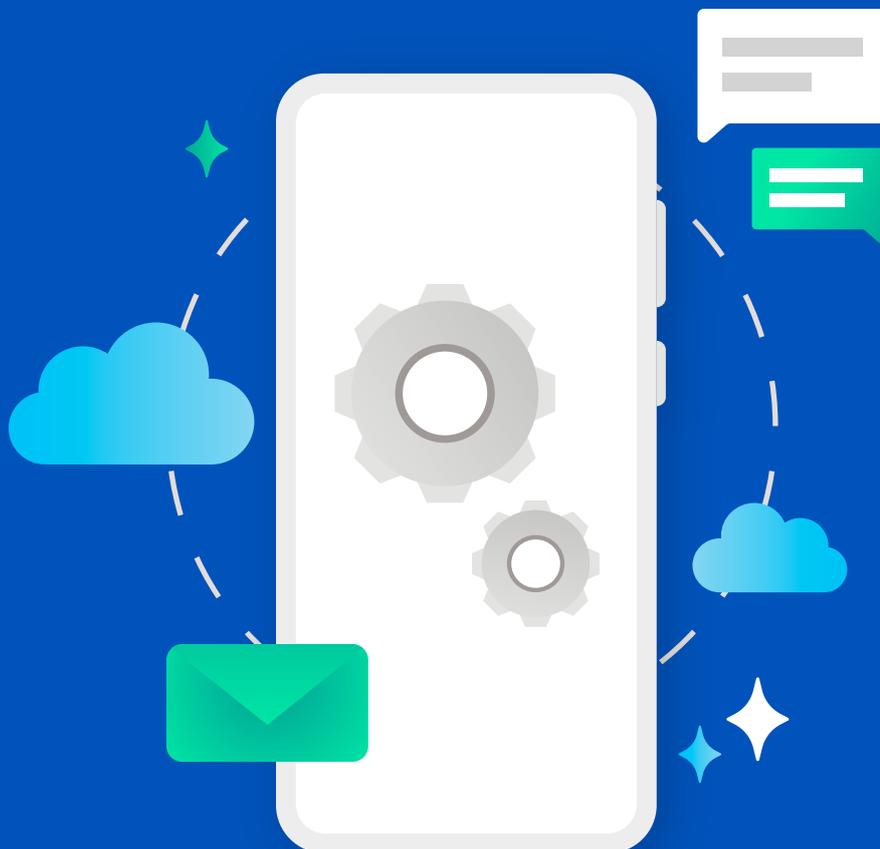


Implementing a Bring Your Own Device policy with your Frontline Employees

A guide on how to deploy a BYOD policy in your organisation to better enable your frontline



Why implement a BYOD policy for your employees?

It is important to give your employees the flexibility to get the information they need on any device they use—whether that's their own device, a POS machine or company tablet.

Introducing a BYOD policy for your business will ensure your organisation can communicate securely with all employees.



Employees have the ability to use IT they feel comfortable with and benefit from individual accessibility options



Your organisation can set up policies and guidelines to ensure that personal and work data remain separate, so all employees have the confidence to work safely and share company data securely



Reduce overhead when procuring and provisioning fewer corporate devices



Provide resilient alternative if workers are unable to access their main places of work

Roadmap to a successful deployment of BYOD policy

1. Establish goals you want to achieve

What are the key benefits your organisation will gain from BYOD? Make sure you can measure and define these.

2. Identify existing policies or create a new one

If you already have an Information Security policy or Working from Home policy, these should be updated to include BYOD.

3. Identify the data users will be able to access on their device

Consider which data can be processed on a personal device and which must be held on a corporate device only – make sure it's clear what is accessible via Teams so expectations are set.

4. Learn whether appropriate security controls are in place

Review the controls you have in place and decide if they are appropriate for any sensitive personal data being processed. Consider enabling services like Multi Factor Authentication (MFA) if you haven't already.

5. Define scope and level of support

Understand how to help your service desk support BYOD users with 'how-to' guides and easy troubleshooting instructions.

6. Create a champions network and communication campaigns

Once you have considered the pre requisites, it's time to build your team to help you deliver the policy and adopt BYOD into your organisation.

Create super users and BYOD champions to help employees understand how to access Teams on their device and how it will improve their ways of working.

Managing personal Devices using Microsoft Endpoint Manager

Using Microsoft Endpoint Manager will allow your organisation to easily, securely and efficiently manage both corporate and BYOD devices for your business. No need to add in any third-party tools or additional licencing – BYOD is ready to deploy when you are!

Security and Compliance on BYOD Devices

Multi Factor Authentication

Secure access management through Multi Factor Authentication on the device or application managed through your BYOD policy

Compliant devices

You can set a policy to ensure that only devices with compliant OS and security updates can access your corporate data

Licencing

If you already have an Intune Licence, Enterprise Mobility + Security or Microsoft 365 you're ready to go!



How to manage the devices

Enrolled Devices

Enrol a personal device into Intune and manage it just like your corporate devices, retaining a detailed level of control on how the device is used whilst accessing corporate services.

Unenrolled Devices

Microsoft Application Manager will enable you to securely deploy applications to an unenrolled device with control over your corporate data with that application. You can containerise the corporate data and keep it separate from personal data within the same Teams app.

Intune device management fundamentals

- Intune App provides a secure, containerised solution that enforces encryption, device pin and checks device health before allowing access to Office 365.
- As soon as someone downloads one of the enabled apps and authenticates with their work account, the Intune App policies will be applied, regardless of whether their device is MDM managed or not.
- There are many apps that can be secured with Intune App Protection policies.

Resources to help start your BYOD plan



What if some of our staff do not have a personal device to access Microsoft Teams on?

If your staff don't have a personal device they can still access their important company communication on shared tablet or kiosk devices in your stores.

What if I don't have a team to develop a BYOD policy?

Bring Your Own Device is simply extending the technology your company is already using for managing corporate devices to include personal devices. By developing a BYOD policy alongside your existing end user compute programmes, you won't need a dedicated team or large number of resources to have a successful adoption of the BYOD policy.

Which applications can be managed by Intune Mobile Application Management policies?

Any app that has been integrated with the Intune App SDK or wrapped by the Intune App Wrapping Tool can be managed using Intune app protection policies.

What is the benefit of Multi identity Support?

Multi-identity support is the ability for the Intune App SDK to only apply app protection policies to the work or school account signed into the app. If a personal account is signed into the app, the data is untouched.

What are the baseline requirements to use app protection policies on an Intune-managed app?

- The end user must have an Azure Active Directory (Azure AD) account.
- The end user must have a license for Microsoft Intune assigned to their Azure Active Directory account.
- The end user must belong to a security group that is targeted by an app protection policy. The same app protection policy must target the specific app being used.
- The end user must sign into the app using their Azure AD account.



Useful Links:

[Technology decisions for BYOD with EMS | Microsoft Docs](#)

[How to have Secure Remote Working with a BYOD Policy](#)

[What is Microsoft Intune device enrollment - Microsoft Intune | Microsoft Docs](#)