

BYOD (Bring Your Own Device)

Guidance for private and public sector organisations considering a BYOD approach

CPNI
Centre for the Protection
of National Infrastructure



Limit the information shared by devices
Staff are used to sharing their information with other users and in the cloud. The automated backup of device data to cloud based accounts can lead to business data being divulged.



Understand the legal issues
The legal responsibility for protecting other people's personal information is with the data controller, not the device owner.



Anticipate increased device support
Your services may need to be accessed by different types of device, so ensure you have the IT support capability and expertise to manage a growing range of devices.

Create effective BYOD policy
Ensure that personally-owned devices are only able to access business data that you are willing to share with authorised staff.



Encourage staff agreement
Communicate your BYOD policy through staff training so they understand their responsibilities when using personally-owned devices for work purposes.

Consider using technical controls
Container applications and technical services such as Mobile Device Management can help you remotely manage personally-owned devices, but they can impact the usability of the device.



Plan for security incidents
When incidents occur, act quickly to limit losses. Could you remotely wipe sensitive data from a personally-owned device if it was lost or stolen?



Consider alternative ownership models
Restricted devices may not appeal to some users, so consider giving staff a choice of approved devices which are purchased and controlled by your organisation.