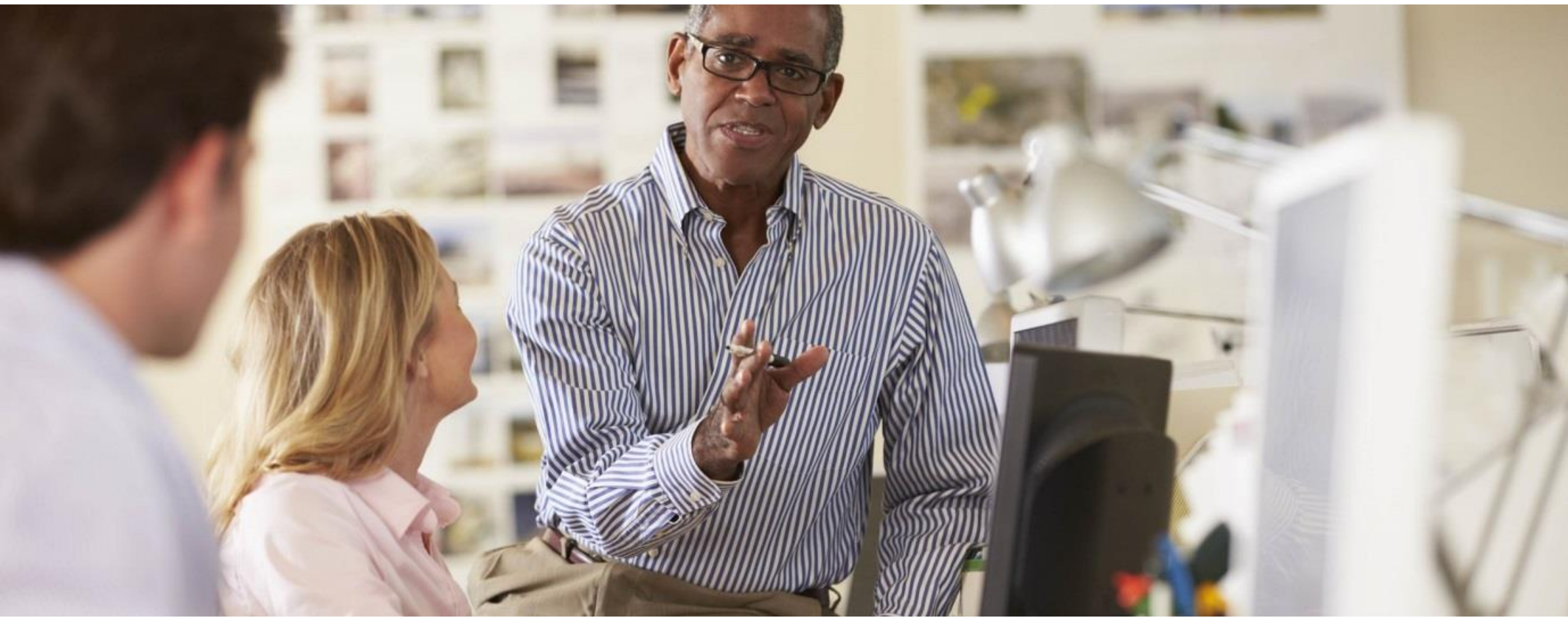
academia
for business



# MDM: Effective use of mobile devices in the workplace

*What do you need to take into account when considering the use of mobile devices for your workforce?*

The last couple of years has seen mobility emerge as one of the key trends in the enterprise IT space. With smartphones and tablets becoming more powerful, there's a growing recognition that they have a major role to play in the business world.

This is partly driven by people's increasing familiarity with these devices in their personal lives. For many consumers, it's just as natural to browse the internet, buy products online and stay in touch with friends and family on a mobile device as a PC, and this trend is only set to grow in the coming years.

For instance, Gartner has forecast that by 2018, the average consumer will use three to four main devices, including a laptop, smartphone and tablet, as well as more niche items like smartwatches. Anshul Gupta, research director at the firm, said: "The combination of the high level of adoption of technology, the availability of faster networks, and decision making becoming increasingly dependent on real-time information, will undoubtedly lead to more devices per user."

## The rise of the mobile workplace

This is a trend that will naturally spill over into the workplace. Figures from Research and Markets suggest the global enterprise mobility market will be worth more than $360 billion (£241.6 billion) by 2020, as more businesses come to recognise the value of the technology.

Meanwhile a study by Appian and Harris Poll found that 90 per cent of IT decision makers say enterprise mobility will be a critical function for customer engagement, competitiveness and operational productivity in 2016.

But there's a lot more to this than simply issuing employees with smartphones, or even letting them use their personally owned items for work purposes. If organisations are to make mobility a success, they need to think carefully about what the implications will be for their business, and what they need to do to ensure that they are not left exposed to the pitfalls that mobility can bring.

## The need for control

In order to stay safe when using smartphones and tablets in a business environment, some form of mobile device management (MDM) solution is essential. This usually consists of third-party applications that are installed on mobile devices and allow the IT department to keep control over what activities take place on them.

For example, it can allow a company to set restrictions on what apps can be downloaded to its employees' devices, as well as what business data individuals will be permitted to view when away from the office's network.

This is vital in protecting company information when it is accessed outside of the business' tightly-controlled perimeter. Mobile malware is a growing threat, but despite this, many individuals do not take the same precautions on their smartphone or tablet that they would on a PC. Therefore, it's vital that businesses have a strong, clearly communicated policy in place to govern the use of these items.

## The right solution for you

The key to choosing the right solution is understanding your unique business needs. A good MDM solution needs to reflect the type of work that you expect to be conducted via mobile devices, as well as the profile of the people using it. With this in mind, here are some key considerations you need to think about.

- **How open should it be?**

MDM tools will typically offer a range of options for restricting usage, from fairly liberal policies that enable users to pick and choose what apps they use, to complete lockdowns which only allow a device to be used for certain activities. Generally speaking, the more sensitive the data you're working with, the tighter the controls that need to be in place.

- **Managing multiple platforms**

A key challenge will be integrating the multiple platforms on offer with mobile devices, with iOS, Android and Windows being the major players. One solution is to restrict which of these employees can use - for instance, by only allowing iOS devices. However, this may not always be practical, so an MDM solution that can work effectively over multiple operating systems is a must.

- **Who's viewing your data?**

Ensuring that only authorised personnel have access to vital information is a key part of an effective MDM tool. Permissions that ensure only the right people have authorisation should be enabled, while this can also help identify potential threats to an organisation by monitoring who is viewing information.

## Finding the BYOD balance

In reality, employees will end up using mobile devices, whether they have express permission from their company or not. Therefore, allowing the use of personally-owned items - so-called bring your own device (BYOD) - is often the best way to bring this technology into the business quickly, cheaply and, most importantly, in a controlled manner.

With the right software, businesses can ensure they can roll out BYOD in a consistent, safe way and take advantage of the higher productivity and improved employee engagement that a strong mobility policy can deliver.

academia
for business

**Academia Ltd**
8 Kinetic Crescent
Innova Park
Enfield
EN3 7XH

| | |
|---|---|
| call | **01992 703900** |
| fax | **08456 120119** |
| email | **sales@academia.co.uk** |
| web | **www.academia.co.uk** |
| twitter | **@AcademiaGroup** |