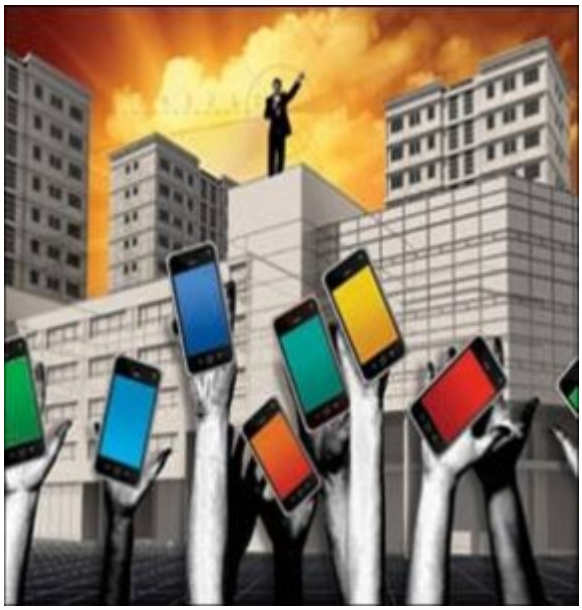
# Practical tips for an effective BYOD policy (Bring Your Own Device)



In this article we highlight the potential risks and benefits for businesses of allowing employees to use their own personal mobile devices (tablets, smartphones, laptops or notebook computers) for business purposes. We talk through the important issues to consider when putting together an effective Bring Your Own Device(BYOD) policy, to maximise the upsides whilst limiting the risks.

Fuelled by the surging use of smartphones, high speed internet services and 4G as well as the growth in remote and flexible working, staff today have come to expect to use their own devices to conduct business. Employers of every size have been quick to adopt a BYOD approach.

Although the following figures are from the USA, the BYOD statistics below show impact of BYOD in the workplace and its widespread adoption.

> The BYOD market is on target to reach nearly $367 billion by 2022, up from just $30 billion in 2014 (Research report by Global Markets Insights Inc 2016).
>
> 59% of organisations allow employees to use their own devices for work purposes. Another 13% had planned to allow use within a year (From Tech Pro Research published in 2016).
>
> 87% of companies rely on their employees using personal devices to access business apps (Research by Syntonic) conducted on a survey of 409 respondents among CEOs, CFOs and CIOs who work for companies with >100 employees,  published in 2016).
>
> As of 2016, six out of 10 companies had a BYOD-friendly policy in place (from the same Research by Syntonic).

## BYOD benefits

BYOD can bring a number of benefits to businesses, including:

> Increased flexibility and efficiency in working practices.
>
> Improved employee morale and job satisfaction.

A reduction in business costs as employees invest in their own devices.

## BYOD risks

The boom in BYOD has been matched with an upsurge in activity by criminals trying to exploit the data and intellectual property stored on personal mobile devices. The use of personal mobile devices for business purposes increases the risk of damage to a business's:

IT resources and communications systems.

Confidential and proprietary information.

Corporate reputation

Customer and employee data
The General Data Protection Regulation ("GDPR") which became law on 25th May 2018, has increased the risks of BYOD through:

enhancing the rights of individuals with regards to their data (e.g right of access, correction, deletion), increasing the legal responsibility on businesses (the data controller in this context) to keep data secure, and allowing the ICO to fine organisations for breaches and non compliance.

Obviously allowing employees to use their own devices to conduct business comes with an increased risk of data breaches, both physical (such as leaving a device on the train) or electronic (such as hacking or malware).

The research cited above showed that even before GDPR came into force, companies and CIOs were well aware of the security implications of a BYOD approach: 61% of respondents in the Syntonic survey viewed mobile devices as less secure than fixed devices such as desktop personal computers, but said that security measures aren't always consistent.

## Ownership of the device

Personal mobile devices are owned, maintained and supported by the user, rather than the business. This means that a business will have significantly less control over the device than it would normally have over a corporately-owned and provided device. But the business remains responsible for protecting company data stored on those personal mobile devices.

## Issues to consider in a Bring Your Own Device (BYOD) policy

A BYOD policy brings with it unique challenges which employers must address, such as:

How will the business record and keep track of the devices used to access company data?

What security measures will be installed on employees' devices?

What are the steps required if a device is lost or stolen?

Will an employee be required to a return a device to the company for wiping on termination of employment?

Are company emails stored on the employee's device? If so particular care should be taken when an employee leaves the business, as company emails and data will remain on their device.

The tone of the BYOD policy should be varied depending on whether the BYOD policy is voluntary (and the employer offers an alternative company-owned device) or whether using their own device is the only option available to the employee. If the policy is purely voluntary, then the employer may impose stricter limitations on usage and more stringent monitoring requirements. If employees are required to use their own device for business purposes, then there is likely to be less scope to impose limitations, particularly if there is an associated cost for employees.

## How to manage the risks associated with a BOYD scheme

To de-risk the business when adopting a BYOD scheme, employers should:

Audit and assess the risks, including assessing:
where the data is held?
what type of data is stored?
how will the data be transferred?
what is the potential for leakage ?
how easily employees may blur personal and business use?
and how cloud-based services will affect security?

Ensure that security measures impose controls on access to data, encryption and PIN numbers, and verify the device's security features.

Keep pace with advances in the features of devices and maintain a list of approved models. Choose Your Own Device (CYOD), is becoming more popular, where employees choose from a list of models pre-approved by the business.

Insert safe and secure deletion methods on the device.
Note that the ICO guidance recommends that portable devices used to store and transmit personal data should be encrypted. A failure to protect data using encryption software may lead to the ICO taking enforcement action against an employer.

Consider how the use of company data on the device can be monitored. The ICO guidance recommends using technology to monitor the device to assess data leakage and loss, but reminds employers to consider employee privacy; a careful balancing act must be maintained and employees should be informed of the monitoring.

Have a well-publicised BYOD policy.

Before implementing a BYOD policy, an organisation should look at the strategic and business case for it, and conduct a privacy impact assessment. In particular, employers should consider:

Compliance with relevant laws – the GDPR 2018 we have already mentioned, and the Data Protection Act 2018. Privacy impact assessments are a legal requirement under the GDPR in some circumstances. Implementing a BYOD policy will almost certainly require employers to carry out a privacy impact assessment.

Whether consultation with any staff forums, employee bodies or trade unions are required before

implementation of a new BYOD policy.

Whether BYOD will save the company enough money, taking into account the potential hidden costs such as employee reimbursement, licensing, infrastructure and support to justify a potential reduction in control over the processing of company data (particularly if employees are using a variety of makes and ages of device which may have varying degrees of security sophistication).

Whether there are any technical limitations to implementing a BYOD policy. An example of this might be capacity restrictions on the internal Wi-Fi network, or a lack of sophistication in the IT team with respect to technical security measures.

# Securing data stored on a device

A business is responsible for protecting company data stored on personal mobile devices. Businesses should consider implementing security measures to prevent unauthorised or unlawful access to the business's systems or company data, for example:

Requiring the use of a strong password to secure the device.

Using encryption to store data on the device securely.

Ensuring that access to the device is locked or data automatically deleted if an incorrect password is inputted too many times.

The business should ensure that its employees understand what type of data can be stored on a personal device and which type of data cannot.

# Mobile Device Management for BYOD

Mobile Device Management software allows a business to remotely manage and configure many aspects of personal mobile devices. Typical features include:

Automatically locking the device after a period of inactivity.

Executing a remote wipe of the device (make sure employees are aware which data might be automatically or remotely deleted and in which circumstances).

Preventing the installation of unapproved apps.

# Monitoring use of a device

Employers should also consider how, and to what extent, they will have access to and monitor company and personal data contained on employees' personal devices. Employees have a reasonable expectation of privacy under Article 8 ECHR. Steps should be taken to ensure that company and personal data are segregated on personal devices, and access to personal data by the employer is minimised.

## Loss or theft of a device

The biggest cause of data loss is still the physical loss of a personal mobile device (for example, through theft or by being left on public transport).

Loss or theft of the device could lead to unauthorised or unlawful access to the business's systems or company data. The business must ensure a process is in place for quickly and effectively revoking access to a device in

the event that it is reported lost or stolen.

Businesses should consider registering devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft.

### Transferring data

BYOD arrangements generally involve the transfer of data between the personal mobile device and the business' systems. This process can present risks, especially where it involves a large volume of sensitive information. Transferring the data via an encrypted channel offers the maximum protection.

Employees should be encouraged to avoid using public cloud-based sharing which have not been fully assessed. Businesses should provide guidance to employees on how to assess the security of wi-fi networks (such as those in hotels or cafes).

### Departing employees

A business needs to think about how it will manage data held on an employee's personal mobile device should the employee leave the business.

## BYOD and the 'Always on' culture

There is increased commentary around the potential negative consequences of remote working and mobile device usage and its impact on employees' wellbeing as a result of the 'always on' culture. Particularly where use of personal devices is voluntary, employers may wish to consider including the optional 'work-life balance' sub-clause in any BYOD policy, to help evidence a commitment to their duty of care towards employees and counter claims in connection with, for example, stress-related illnesses from employees.

## BYOD and registering employees' devices

A key aspect of an effective BYOD policy is ensuring that the employer is aware of the data processing activities that are being conducted in respect of company data. To mitigate against the risks of unlawful processing and undisclosed data breaches, employers should require all employees to register their devices with the employer before using it for business purposes. Employers should also take this opportunity to set up the device with appropriate security software, and register it with remote locate and wipe technology in the event a device is lost or stolen.

## BYOD and unauthorised access and repairs

There is a risk of data breach if an employee arranges for a device to be repaired by an unknown third party who may be able to access company data. Requiring that all repairs are arranged through the company will allow for greater control over who has access to the device. If this approach is adopted, the company should also meet or contribute to the cost of repairs. Therefore, the company must balance the costs of contributing to repairs against the risks of a data breach.

## ICO guidance on BYOD

The Information Commissioner's Office has published guidance on bring your own device and the data protection issues for employers who adopt a BYOD approach. The guidance has not yet been updated to take into account GDPR but many of the practical points it makes are still valid and useful. It highlights:

the importance of  having a clear BYOD policy that is regularly audited and monitored for compliance

that staff connecting their devices to the company IT systems fully understand their responsibilities

that alongside a BYOD policy, employers create and maintain an Acceptable Use Policy (to provide guidance and accountability of behaviour) in order to minimise the risk of unauthorised or unlawful processing of data or the accidental loss or destruction of personal data.

## NCSC guidance on BYOD

The National Cyber Security Centre, part of GCHQ, has published a useful infographic as part of its summary of the key security aspects for large and public sector organisations.

Choose Your Own Device (CYOD) is likely to offer employees an advantage to select one among several enterprise-approved systems and this is predicted to eliminate standardization and security challenges of BYOD system.

This article seeks to spotlight the key issues around BYOD and how adopting a BYOD approach may affect your business and HR practices.