

torrwaterfield



ACCOUNTANTS & BUSINESS ADVISORS

TELEPHONE: 0116 242 3400 | FAX: 0116 242 3401 | EMAIL: INFO@TORRWATERFIELD.CO.UK

WWW.TORRWATERFIELD.CO.UK

Bring your own device (BYOD)

Some employees will often prefer to use their own personal mobile devices to access company networks/systems. However, this is potentially a security loophole which places the organisation at risk from reputational damage and legal proceedings.

Firms need to have a formal policy with regard to the use of personal devices at work.

Bring Your Own Device refers to this type of policy - which defines what mobile devices (if any), employees can use to access company networks/systems.

We consider how to structure such a policy, and what it may contain.

Broadly what should a BYOD policy cover?

Firms need a policy which sets out the devices which may or may not be connected to a firms' network; procedures to ensure that non-approved devices can never be 'accidentally' connected; and appropriate mechanisms in place to maintain security over personal data which may be stored on mobile devices.

Audit of existing devices and access rights

The first step is to perform an audit of the current situation. Which devices use the network, and what for?

What does the law say?

As the employer (who is the data controller) there are obligations under the Data Protection Act 1998 (DPA) to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

There is a high risk that confidential corporate and client data can find its way onto personal devices - which are usually not very secure and can be easily lost/misaid/stolen.

The risks of reputational damage

Imagine the scenario, an employee receives an email with an attachment containing a mailing list of all clients and their contact details which they open and save onto their mobile device. If that device then goes missing the data stored on it could find its way into the public domain, or be mis-used, or sold onto a competitor. What's worse is that the ICO will need to be notified of the loss of data, as will each individual on that mailing list. This can cause major reputational damage as well as a large financial penalty.

Which devices are acceptable?

Having performed an audit, the second stage is to decide what to include or exclude from a BYOD policy, and this is usually done at device level.

Level	Device
1	No devices (zero-tolerance)
2	A list of 'approved' devices
3	Any/all devices

1 - Zero-tolerance

This may be the quickest, easiest and simplest solution, but may not necessarily be the most pragmatic or practical.

It may also serve to hinder rather than help some employees perform certain tasks, which can lead to job dissatisfaction and a lowering of morale.

So an outright ban could prove to be counter-productive.

It can also be quite difficult (and therefore expensive) to control and police a zero-tolerance policy without strong network security controls.

2 - Approved devices

This allows a set list of devices, or, devices with particular operating software (e.g. iOS devices only or Android and Windows devices only).

The approved device approach can make it easier to manage and control access, but may leave some employees disadvantaged if their device is not covered. It can also be difficult to manage, as new models and new devices emerge on a daily basis.

3 - Any device

This allows any device to be 'plugged in'.

This approach is entirely opposite to zero-tolerance and allows any device to be 'plugged in' at any time. Advantages are a) for the employee who is not restricted by device, and b) for the company which does not have to keep updating a list of approved devices.

However, strong controls such as mobile device management systems need to be employed with this type of approach.

An alternative option!

In an increasing trend, some firms have decided to abandon BYOD and have a zero-tolerance policy, in favour of providing devices to employees.

Which applications are acceptable?

The firm may wish to restrict access to certain applications – most often to email and internet access only. Full blown access to networks and applications should be avoided where possible, other than from PCs or laptops and then only via trusted intranets or secure remote access tools.

Business v. private use

BYOD devices owned by an employee are likely to be used for both business and private purposes.

On the one hand the employee has to be confident that the company will not access personal material stored on the device or use device monitoring tools, whilst on the other hand the company will want to protect corporate and client confidential information which may also be stored (or visible) on the device.

Employers also need to be aware that devices may be used (for personal purposes) not just by the employee, but also by other family members.

Wireless security

The easiest and quickest way for devices to be attached to a network is for employees to use their device to login to a network, wirelessly. Some firms publish their wireless key to employees without realising that they are using the key on all devices including personal devices.

So, one of the cheapest methods of providing device security is to make the wireless key very strong (i.e. difficult to remember), only available on request and only entered into the device by a member of the IT support team or other nominated individual. Thus control can be maintained at device level relatively easily.

Device registration

Most current versions of network operating software (Windows and Mac) have inbuilt security tools which can be used to maintain a list of 'approved' devices.

This is done through a registration process whereby the device is presented and registered on the network.

If a device gets mislaid or an employee leaves, the device can be blocked/removed from the list of registered devices.

Mobile device management (MDM)/Mobile applications management (MAM)

A more expensive way of providing device security is to use MDM services – these may either be provided as part of the network operating software, or this service may be provided by a third-party.

There are different levels of this type of service ranging from simple registration and device reset services, to sandboxing personal and corporate data – which will allow separate wiping of corporate data only.

Employees will have to agree/consent to whichever mobile device management system is used if they want to adopt BYOD.

Employees must also agree/consent if MDM software is used to monitor the device, the activities which are monitored and whether or not geo-location is used.

Finally, employees will need to understand what will happen to their own personal data stored on the device, in the event the device has to be disabled.

Data encryption

A BYOD policy in itself is not enough to provide sufficient safeguards. All confidential/personal data must be encrypted. Just setting a document/spreadsheet as read-only, or creating a password to open the document/spreadsheet is not the same as encrypting the data.

Firms must assess what personal data is being transferred from and to which devices, perform a risk assessment of the chances of the data getting into the public domain, and then use appropriate encryption methods to protect that confidential/personal data.

Other issues to consider

- Device password protection - Each BYOD device must have a start-up password/pin and should lock if not active for a specified number of minutes

- Misplaced devices – as part of the BYOD policy the employee will need to know who to contact and what will happen to the device if it is misplaced (i.e. what data might be wiped from the device)
- Cost – the firm may or may not agree to pay for certain mobile device charges
- Acceptable use policy – the firm will want to ensure that any acceptable use policy also applies to BYOD devices
- Devices which have been rooted/jail-broken should not be permitted
- Storage media – the firm may want to specify the approach with regard to memory/SD cards.

Implementing the BYOD policy

BYOD can either be formulated as a separate policy, added to an existing acceptable use policy, or added to an existing Internet and email policy or social media policy.

Company devices, by default, will come under the scope of BYOD.

Employees with their own personal devices should be given the opportunity to opt-out or opt-in to the BYOD policy -

- Opt-out - Decline to sign-up for the BYOD policy – in which case the employee will not be able to use any personal devices for work.
- Opt-in - Agree to sign-up for the BYOD policy – in which case their device will need to be registered on the network and also, if applicable, with a mobile device management service.

See our summary for our 4 easy steps in defining and implementing a BYOD policy.

Summary

It is important that the employer (who is the data controller) remains compliant with the DPA with regards to the processing of personal data. In the event of a security breach, the employer must be able to demonstrate that all personal data stored on a particular device is secured, controlled or deleted. Having a BYOD policy will go a long way towards meeting that objective.

4 steps to defining and implementing a BYOD

Step 1

Audit devices and usage

What devices are currently allowed onto the network?

What access rights do they have?

What applications do they use?

Step 2

Level of BYOD

Decide which level of BYOD is to be adopted –

1. No devices
2. Approved list
3. All/any devices
4. Define which applications are accessible to mobile devices

Step 3

BYOD policy

Formulate and write the BYOD policy.

Make appropriate network infrastructure security changes and procure any additional services (such as MDM).

Decide if additional security is required such as data encryption tools.

Define and communicate a date for implementing the policy.

Step 4

Implementation date

Remove all current devices.

Register approved devices.

Employees who own such devices sign BYOD.

How we can help

Please contact us if you require help in the following areas:

- Performing a security/information audit of corporate/client data and who and what access this data
- Defining a BYOD policy
- Implementing a BYOD policy and training staff.