# Bring your own device (BYOD)

*This Guidance Note was written by the LexisNexis team.*

***For the duration of the COVID-19 Level 4 lockdown period, all non-essential workers are required to work from home until further notice. While some staff may have access to firm-owned IT equipment, such as laptops, tablets or desktop hardware, many others are reliant on personal computer equipment to access vital systems, software and documents.***

***Since the announcement of Level 4 restrictions, many firms have quickly implemented interim solutions to facilitate the continuation of normal working with minimal disruption, setting up workers with remote access or other tools.***

***As the COVID-19 pandemic develops, and firms begin to look ahead to potential long-term home working, this Guidance Note outlines a range of considerations necessary for establishing policies and processes for the ongoing use of personal IT equipment when accessing and handling sensitive firm and client information.***

***This Guidance Note focuses on BYOD in the employment relationship.***

## *Key risks and benefits of BYOD?*

'Bring your own device' (BYOD) refers to arrangements where an organisation allows designated employees to connect to its corporate IT network using their own communications devices, for specific, work-related purposes. These arrangements will most commonly apply to use by staff of their personal devices for work. However, the term 'BYOD' may also be used in other situations, such as access to an educational institution's network by its students or access to an organisation's network by its customers or business partners, as a way to exchange and update information. BYOD arrangements may cover a range of devices, including laptops, tablets and smartphones.

| Key risk or benefit | Potential benefits | Potential downsides and risks |
|---|---|---|
| **Availability** | During the COVID-19 pandemic, there may be increased demand for corporate IT equipment and a reduced supply and/or delays in fulfilment and shipping.<br>Getting equipment to those that need it (and ensuring it is properly set up) is significantly more challenging than usual. Staff using existing personal equipment avoids this logistical challenge. | Multiple members of one household may be competing for shared computer equipment meaning staff could face limited hours of use.<br>Available devices may be of a different operating system or specification than those used in the office. Staff may be unable to source alternative equipment so processes may need to be adapted. |
| **Cost savings** | There is a cost saving for the organisation:<br>—in not having to invest in procurement, replacement and management of devices for employees<br>—depending on the arrangements for sharing costs, in relation to service charges (where employees may be compelled to use devices more responsibly) | The organisation will still need to make some investment in a technical solutions, training and support to enable BYOD access by employees (which may in some cases make it more expensive)<br>If an organisation stops buying devices for employee use under existing contracts with their communications provider (which often bundle a range of products |

| | | |
|---|---|---|
| | | and services together), this may impact discounts received on other product/service lines. It is important, therefore, to review existing supply contracts before implementing BYOD |
| **Flexibility** | BYOD is a potentially effective response to changing ways of working that enables employees to be more flexible and mobile | Organisations have less control over employee devices and there is an increased risk of a device containing company information being lost or stolen, particularly on public transport or in other public places |
| **Productivity** | Employees' familiarity and comfort with their own devices can mean they are more productive<br>Staff may be more likely to work ‘out of hours’, eg checking and answering emails or phone calls | Employees being able to readily access personal apps on the same screen as work programs may be a distraction<br>Employees may not be happy to be available ‘out of hours’ |
| **Employee satisfaction** | Employees are potentially happier when using a device that they presumably like (since they bought it in the first place) | Employees' personal financial circumstances need to be considered when it comes to timing of device upgrades<br>Some employees may not feel comfortable using their own devices for work purposes. They may also perceive (eg if work emails etc are accessed on their personal device) that this will encroach on their personal time and affect their work/life balance |
| **Device quality and 'newness'** | Some employees may be more likely to invest in the latest devices (whereas organisations tend to buy the most basic model that delivers the required functionality at the best bulk buying discount) | Those employees who are less likely to invest in the latest technology may find their outdated devices are not fit for purpose |
| **Device care and support** | Employees may be more inclined to take better care of and troubleshoot their own devices than company-owned devices | Loss or theft may be more likely to in relation to a personal device that the employee takes with them everywhere than a company device that will usually be left at work |
| **Information security** | Technological advances are reducing some of the security risks typically associated with BYOD, eg solutions that ensure company information is not stored locally on an employee's device and data wiping technology<br>Given some employees are will be using their own devices for work anyway, by setting up BYOD properly, organisations can at least ensure this is managed more effectively | There are security risks associated with employees accessing the corporate network and potentially saving company information locally on their devices<br>There is the potential for financial loss, legal liability and brand damage to organisations arising from security breaches or data losses involving employee devices<br>Additional measures may be needed to demonstrate that BYOD arrangements comply with |

| | | |
|---|---|---|
| | | regulatory requirements (which may carry a cost for the organisation).<br>There are also the practical issues of enforcing rights to audit employees' devices<br>There is the potential for employees' devices to infect corporate network with viruses or malware<br>Employees’ approach to security when using their own devices may be more relaxed, eg they may be happy to let family members use their own device, or provide credentials (including passwords) to a third party for maintenance or repair |
| **Employee data and personal privacy** | The company may install security measures that better protect the employee's device from viruses and hacking, etc than they would have themselves | In return for being able to use their own devices, employees will generally have to be prepared to accept a certain level of intervention or intrusion by their employer<br>An employee’s expectation of privacy may be higher when using their own device<br>Data wiping technology does not necessarily discriminate between company information and employees' personal data |

Consider also the tax implications of BYOD arrangements, eg where the employer contributes towards the cost of the device or usage costs.

## *Protecting against security risks*

There are some basic steps an employer can take to protect against the security risks inherent in permitting BYOD.

### Develop and implement a BYOD policy

Organisations that permit BYOD should have a defined policy governing its use, to which employees sign up as a condition of using their own device under BYOD arrangements. A BYOD policy should clearly:

- set out that all company information belongs to the employer
- set out the overarching policy objective, ie protection of company information—any rights or obligations under the policy should be directed towards achieving this objective
- define who is covered by the policy
- specify the devices covered by the policy—decide which devices and operating systems will be supported (and ensure this can evolve over time) and implement a device registration procedure
- define who owns what in terms of data and apps
- outline what technical support the organisation is prepared to give and the limits on this
- set out employees' obligations, eg regarding security measures (ie passwords), costs of repairs, back-ups of data, permitted apps/non-permitted activities (eg 'jailbreaking—a process that may remove some of the default security controls an operating system has in place'),

segregation of personal and work data and compliance with requests by the organisation to audit their device

- privacy expectations and details of any monitoring that will take place
- how to report the loss or theft of a device
- the consequences if the employee does not comply with the policy, the employee's device is lost or stolen or the employee stops working for the organisation

An organisation's existing policy on acceptable use of corporate technology can form a useful starting point for developing a BYOD policy. The BYOD policy will also need to dovetail with the organisation's broader information security policy.

### Staff education and training

Training can be a useful way of ensuring that staff fully understand the objectives of the BYOD policy, the rules and restrictions placed on BYOD use and potential consequences of non-compliance. Employers should ensure that employees are fully aware of their obligations and the procedures in place to protect company and personal information.

### Encourage employees to adopt responsible security behaviours

Because devices are employee-owned and controlled, organisations will need to rely on employees to take primary responsibility for the security of their devices. Employees should be required to implement passwords or lock screens for their personal devices. Such passwords should be strong and not easily bypassed, and ideally there should be separate password verification for each service accessed. These requirements should be incorporated in the BYOD policy, to which the employee signs up, and enforced practically when the employee registers their device.

Organisations may wish to build into their BYOD policy some guidelines for employees on acceptable use, particularly as the line between work and personal use may easily become blurred if an employee is using the same device for everything. However, organisations should not be excessively prescriptive about what employees can and cannot do with their own devices (particularly in their own time), and such guidelines should therefore be confined primarily to:

- activities that present a real security risk to the organisation
- reminding employees that they should behave no differently than they would on a work device in terms of the content they can view and how they treat other employees, and
- the action that may be taken by the company if an employee (inadvertently or not) transmits inappropriate material over the company network or transmits company information via social media, email or other personal channels

Organisations will also need to determine how, practically, they will get employees to install company-prescribed apps and updates.

### Incorporate BYOD deregistration with HR processes on exit

Consider how employees will be deregistered from the BYOD platform when they cease working for the organisation. This may involve removing access tokens, disabling email and/or web portal access and checking employee devices to ensure locally-saved company information and company apps have been removed as part of the standard HR exit process. However, if the circumstances of departure are fractious or no formal exit interview is held, this may be difficult to enforce.

Therefore, organisations should ensure they have a back-up plan for removing access to the company network by former employees or other users and safeguarding company information by remote means if the departing employee does not cooperate. Measures such as (non-selective) remote data wiping should be used only if this is reasonably necessary and is a proportionate response in light of the information security risk posed to the organisation.

Employers may also wish to consider deregistering employees:

- temporarily, during suspension
- during garden leave

## *Choosing the right technical solution—security*

A range of technical models can be used for BYOD. The main considerations influencing the solution ultimately chosen by the employer will be:

- cost
- technological capability of existing company IT systems
- support requirements
- how employees need to be able to work and what systems they need access to via non-company devices
- regulatory requirements, (depending on which industry the company and/or its customers operate in)
- security, ie ensuring the organisation maintains network security and control over company information being accessed via personal devices

### Direct network access and local copies

Permitting employees to access the company network directly from, and/or save company information onto, their personal devices, is not particularly secure. Additional protections will be needed to ensure the company can contain potential information security breaches or data losses.

In this scenario, organisations could:

- contractually oblige employees to co-operate in deleting company information from their devices on the occurrence of certain specified events (eg the device being lost or stolen), and/or
- encourage employees to adopt certain security measures and data management best practice, such as regularly backing up their personal data on their own devices and ensuring that company information is stored only in designated areas/folders on their devices

However, there will always be the issue of how an organisation can enforce this in practice when it needs to contain an information security crisis quickly and effectively (see 'Remote data wiping' below).

### Virtualised or containerised access

If company information on company IT systems is accessed via a web portal, where core applications are virtualised, and no local copy is saved on the employee‘s device:

- the information security risk to the company is significantly reduced, and
- there is generally no need for the employer to monitor the employee’s device or the data on it (see below: *Monitoring employees and/or remotely accessing employees' devices,* or to carry out data wiping see ‘Remote data wiping’ below)

Where there is a need for employees to work agilely and remotely, the use of private clouds by companies to support BYOD is proving an increasingly popular solution.

Emerging models such as secure containers are also enabling better segregation of employee data from company information, meaning that restrictions on functionality such as printing, copying and pasting can be imposed selectively on data within the work container, and a gateway can be imposed to prevent unauthorised apps from opening files stored in the container.

### Connection and tracking

Technical measures can be implemented to ensure that only authorised employees can connect to the corporate network and also to track what data is being copied onto a employee's device (assuming such copying is technically possible). See below: *Monitoring employees and/or remotely accessing employees' devices.*

Software also exists that locks down a device to prevent employees from installing any unapproved apps on the device, but it may be unrealistic to expect an employee to accept this on a device they have paid for.

### Remote data wiping

Remote data wiping technology can enable an organisation to remotely wipe employee devices of company information if there is a data security issue. The problem is that generally this enables data on devices to be wiped only on an all-or-nothing basis, meaning that the employee’s own data and apps will also be lost. However, more discriminate wiping of data is becoming possible, eg if containerisation is used (see above).

See below: *Monitoring employees and/or remotely accessing employees' devices.*

## *Monitoring employees and/or remotely accessing employees' devices*

One of the main practical issues with using BYOD is that it is not always easy to neatly separate company information from personal information on an employee's device. See above: *Choosing the right technical solution—security*.

The technical basis on which employees are granted access to company IT systems is important—an organisation will generally only need to consider measures such as remote access and/or data wiping if a local copy of company information is stored on an employee’s personal device. See above: *Protecting against security risks.*

The need to safeguard organisational information security will always have to be balanced against the individual rights of the employee. From the employee's perspective, data protection, personal privacy, human rights and employment law considerations may come into play.

## *Loss of employees' data*

Where data wiping technology is used, this will not generally work selectively but will wipe all data on the employee‘s device, including personal data (eg contact lists), photographs and other media (eg music) and apps for which the employee has paid.

Organisations will therefore need to consider carefully the circumstances in which they will use (non-selective) data wiping and, if so, what assistance (if any) they will give to employees to help restore their own content on their devices. It would be difficult to justify the use of indiscriminate data wiping unless:

- there was a serious and immediate threat to organisational information security that could not reasonably be dealt with by other means, and
- the organisation had taken reasonable steps to minimise loss to employees' data

Reasonable steps to minimise loss to employees' data may involve preventative action (eg encouraging employees to regularly back up their own data) and/or restorative action (eg providing support to employees to restore content onto their devices or replacement devices).