Bring your own device (BYOD)

Last reviewed: May 2020

Authored by the LexisNexis Legal Writer team.

This guidance note outlines a range of considerations necessary for establishing policies and processes for the ongoing use of personal ICT equipment when accessing and handling sensitive firm and client information.

This guidance note focuses on “Bring you own device” (BYOD) in the employment relationship.

What is BYOD?

“Bring your own device” (BYOD) refers to arrangements where an organisation allows designated employees to connect to its corporate ICT network using the employee’s own devices, for specific, work-related purposes. These arrangements will most commonly apply to employees who use 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, to exchange and update information. BYOD arrangements may cover a range of devices, including laptops, tablets and smartphones.

Key risks and benefits of BYOD?

Key risk or benefit	**Potential benefits**	**Potential downsides and risks**
Cost savings	There is a cost savings for the organisation: • in not having to invest in procurement, replacement and management of devices for employees; and • depending on the arrangements for sharing service charges as between the organisation and employee, as employees may be compelled to use devices more responsibly if costs are shared proportionally. There may also be a benefit for the employee: • in being able to claim a tax deduction for work-related use of the device.	The organisation will still need to make some investment in a technical solutions, cyber security, training and support to enable BYOD access by employees (which may in some cases make it more expensive). 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. There is also an increased risk of inappropriate use of corporate software and systems by the employee, other members of the household, etc.

Productivity	Employees' familiarity and comfort with their own devices can mean they are more productive.	Employees being able to readily access personal apps on the same screen as work programs may be a distraction. Employees' device may not be completely suitable for the company's work. This may lead to non-functioning, slow work programming or time wasted on technical glitches.
Employee satisfaction	Employees are potentially happier when using a device that they presumably had a choice in opting for (since they bought it in the first place).	Employees' personal financial circumstances need to be considered when it comes to the choice made during the purchase of the device and timing of device upgrades. 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 may not be in a financial position to invest in the latest technology may find their outdated devices are not fit for purpose. Alternatively, appropriate devices may not be available or difficult to source.
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 the workspace. There may be uncertainty regarding responsibility to take care of, maintain and repair BYOD devices, as between the organisation and the employee. Assuming, in most cases responsibility lies with the employee as owner of the BYOD device, there may be varying degrees of rigour, depending on financial resources, warranty terms, etc.
Information security	There is a risk for organisations with regards to information security when employees use their own devices. However, some of these risks can be mitigated with the advancement of ICT, such as the creation of a separate work network on a BYOD (eg, using Citrix and cloud-based technology), which allows for employees to continue working without any of the organisation's data being stored directly on the employee's device. Given some employees will be using their own devices for work, by setting	There are security risks associated with employees accessing the corporate network and potentially saving company information locally on their devices. There is the potential for financial loss, legal liability and brand damage to organisations arising from security breaches or data losses involving employee devices. Additional measures may be needed to demonstrate that BYOD arrangements comply with regulatory requirements (which may carry a cost for the

	up BYOD appropriately, organisations may ensure this is managed more effectively.	organisation). There are also the practical issues of enforcing rights to audit employees' devices. There is the potential for employees' devices to infect corporate network with viruses or malware, particularly if the BYOD device is used by others. 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. Also, consider whether legislation such as the *Privacy Act 1988* (Cth), *Archives Act 1983* (Cth) and *Freedom of Information Act 1982* (Cth) applies to the organisation. Certain laws can affect whether an organisation is able to implement BYOD in their environment, and, if so, what compliance measures need to be implemented to ensure all legal obligations can be fulfilled. Additional compliance measures can also add additional costs.
Employee data and personal privacy	The company may install security measures that better protect the employee's device from viruses and hacking, etc than the employee would have installed 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. An employee's expectation of privacy may be higher when using their own device. This may not be the case, particularly in the event of an investigation, Freedom of information request or incident response activity. Data wiping technology does not necessarily discriminate between company information and employees' personal data. Inadvertent damage to an employee's personal data may increase liability risk to an organisation.

It is also important to consider 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 the use of BYOD should have a defined policy governing its use. Employees would be required to agree to the policy as a condition of using their own device(s) under the BYOD arrangements.

A BYOD policy should clearly:

- state that all company information belongs to the employer;
- set out an overarching policy objective, ie protection of company information and 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;
- clearly define what data and apps are owned by the organisation;
- outline what technical support the organisation is prepared to give and the limits on these;
- set out all of the employees' obligations regarding security measures (eg 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;
- set out privacy expectations and details of any monitoring that will take place;
- provide instructions on how to report the loss or theft of a device; and
- state the procedures and 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 agrees to 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). Further, the security of the device and company data stored on that device relies to a large extent, on the co-operation of the employee, so organisations should be mindful of keeping employee’s ‘on-side’. 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

It is important for employers to consider how employees will be de-registered 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 co-operate. Measures such as (non-selective) remote data wiping should be used only if this is reasonably necessary and is a proportionate response considering the information security risk posed to the organisation.

Employers may also wish to consider deregistering employees:

- temporarily, during suspension; or
- 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); and
- 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 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 an employee's device (assuming such copying is technically possible). See Monitoring employees and/or remotely accessing employees' devices below.

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 Monitoring employees and/or remotely accessing employees' devices below.

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 Choosing the right technical solution — security above.

The technical basis on which employees are granted access to company ICT 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 Protecting against security risks above.

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 may not generally work selectively but may 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 carefully consider 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).

Legal considerations

Privacy Impact Assessments (PIA)

Organisations required to comply with the Privacy Act and implement "privacy by design" are encouraged to employ Privacy Impact Assessments (PIA's) for all 'new projects'. This term is used loosely and is intended to cover the full range of activities and initiatives that may have privacy implications, including:

- policy proposals;
- new or amended legislation
- new or amended programs, activities, systems or databases;
- new methods or procedures for service delivery or information handling; and
- changes to how information is stored.

Given the breadth of this definition and the privacy implications, a PIA for the implementation of BYOD across and organisation should be considered as best practice.

See *Office of the Australian Information Commissioner (OAIC): Guide to undertaking privacy impact assessments*

and *Planning and Implementing New Projects*.

Workplace Monitoring and Surveillance

The Privacy Act will apply where monitoring generates information relating to an identifiable individual (eg a particular employee or customer). The Privacy Act imposes various obligations, including obligations to inform individuals that data relating to them is being gathered via monitoring of IT and communications systems and the reason for this.

The Privacy Act does not specifically cover surveillance in the workplace, other than potentially, the products of that surveillance (eg CCTV video recording or a computer record of emails that do not directly relate to the employment relationship). However, an employer who conducts surveillance or monitors their staff must follow any relevant Australian, state or territory laws. This includes laws applying to the monitoring and recording of telephone conversations. Generally, state laws cover the installation and use of CCTV, and some states also have specific workplace surveillance laws, which may cover an array of remote access technologies.

See *Surveillance Devices Act 2004* (Cth), *Workplace Surveillance Act 2005* (NSW), *Surveillance Devices Act 2007* (NSW), *Surveillance Devices Act 1999* (Vic), *Surveillance Devices Act 2016* (SA), *Listening and Surveillance Devices Act 1972* (SA), *Surveillance Devices Act 2007* (NT), *Surveillance Devices Act 1998* (WA), *Invasion of Privacy Act 1971* (Qld), *Listening Devices Act 1991* (Tas), *Workplace Privacy Act 2011* (ACT) and *Listening Devices Act 1992* (ACT).