Bring Your Own Device (BYOD): an employer’s checklist

Summary and implications
A YouGov survey, published last month, found that 47 per cent of UK adults use personal mobile devices, such as iPhones and tablets, for work purposes. However, it also found that only 23 per cent of employers formally regulate their use at work.

There are a number of advantages in allowing staff to use personal devices for work. Increased flexibility, convenience, accessibility, productivity and higher morale are but a few. However, the practice also carries a number of real business risks, given that the device is owned by someone other than the employer.

How you approach the issue of BYOD depends on the nature of your business, whether the practice offers you any real benefits, as well as your IT budget and capabilities. Ideally, you should look at this issue together with your legal advisers, HR and IT teams. Once your direction is clear, decide whether to adopt a formal policy (which may be linked to internal disciplinary, data protection and social media policies) or simply rely on technological solutions. Either way, we suggest you focus on the following three issues:

• **Protect sensitive and confidential business information.** BYOD usage means business information moves outside your IT system. You must retain ultimate control of the type of information employees access, how and where they access it and how secure the information remains.

• **Comply with your data protection duties.** Under the Data Protection Act 1998 (DPA) you remain liable for how personal data is processed and used. It is immaterial that an employee owns the device from which data is accessed. Take all appropriate technical and organisational measures against inappropriate processing and retention of personal data as well as any accidental loss, destruction or damage to it.

• **Keep associated costs under control.** Be clear about who bears usage-associated costs, including day-to-day voice and data charges, technical support and repairs, roaming and apps installation costs as well as recovery of any personal content which may be lost.

Ask a question
If you have any questions please contact:

Michal Stein, Employment Knowledge Lawyer
T +44 (0)20 7524 6510
m.stein@nabarro.com

or

Belinda Doshi, Data Protection Partner
T +44 (0)20 7524 6200
b.doshi@nabarro.com

To view a copy of our recent Technology and Privacy briefing on BYOD, [click here](#)

To view a copy of the Information Commissioner’s Office guidance on BYOD, [click here](#)

The Employment team
To find out more about the team, and our capabilities [click here](#)
**Keep your confidential information secure: decide the “who”, “what”, “how” and “why” of BYOD usage**

BYOD makes no sense if it compromises your confidential information. For this reason, you must decide in advance whether to permit BYOD and if so, the appropriate safeguards to put in place.

As ever, your employees must appreciate what business information is confidential and how they may use it. As the risk of misuse and inadvertent leakage of confidential information increases with BYOD usage, you need to decide early on:

1. The nature of BYOD access you allow: will employees be limited to remotely connecting to your IT systems or will they be able to save data on their own devices?

2. What devices may be used? Not all devices can connect to your IT system and different devices offer different levels of security and anti-virus measures.

3. The type of information which may be accessed using BYOD: firewall or otherwise secure information that is “off-limits”.

4. Who may access the information. Do you limit access to employees only? May agency workers, contractors or consultants use BYOD? And, within the categories of permitted users, do you limit access to certain categories of information, e.g. depending on roles or seniority? How to do you plan to deal with third party usage of the device (e.g. family members)? One option may be to require business information to be stored in a certain way and have access limitations (e.g. password requirements).

5. How information will be accessed, used, stored and retrieved. Determine the necessary protections (e.g. regularly changed passwords, pin numbers, encryption etc.). For example, you may prohibit the use or downloading of personal data (such as names and addresses) onto mobile devices. Adopt sophisticated security mechanisms.

6. How are you going to deal with data leakage, whether accidental or intentional? Consider registering all BYODs with a mobile device management system which allows you to remotely wipe out data. Ensure you have robust monitoring and access rights.

7. The need to terminate data access and use once the employment relationship breaks down or is terminated, or the device is sold or taken for repair. Ensure you can physically access the device and have remote deletion capabilities.

Finally, bear in mind that you are going to want to retain ownership of any information created or used on a BYOD. If necessary, amend your contracts of employment and policies to reflect this.

---

BYOD usage means:

The practice of employees and other staff using their own personal mobile devices (e.g. smartphones, tablets or laptops) for business purposes, either while at work or elsewhere, and either during working hours or non-working hours.

---

A well-drafted BYOD policy will help protect your IT system, reduce the risk of deliberate or accidental loss of confidential information and minimise reputational damage.

Make sure you continue to retain ownership of any information created or used on a BYOD – amend your contracts of employment and policies to reflect this.
You remain in control and liable for all personal data processing:
however and wherever it is carried out

Many of the issues you consider in relation to confidential information are also relevant for data protection. The crucial point to remember is that you, the data controller, have the ultimate responsibility for data protection compliance by all those who access your personal data.

This means you must ensure that any employee who processes personal data complies with the DPA’s principles and that you do the same when accessing personal content of the employee or others on his/her BYOD.

In particular, bear in mind the three obligations to:

- take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data;
- only process personal data for the purposes for which it was collected; and
- not retain personal data for longer than is necessary.

Specific steps you should consider taking to comply with the DPA include (in addition to the steps noted under the confidential information section) the following:

1. Specifically, identify the data you are willing to have accessed via BYOD and the individuals who may access it. You may well decide to prohibit any access or downloading of personal and sensitive personal data onto BYODs and, if so, adopt suitable technical solutions. If you allow access to such data, then consider very carefully by whom, where and via what channels (e.g. only an encrypted channel such as VPN)?

2. If you require all traffic containing personal data to pass through an encrypted channel, such as VPN, consider the monitoring opportunities this provides you and make sure you have employees’ explicit consent to monitoring. Be very clear if you intend to monitor usage by family members or other persons with access to the device.

3. Remind employees that they may only use personal data for corporate purposes. Ensure sanctions are appropriate to deal with intentional as well as inadvertent breaches. Provide appropriate training on a regular basis.

4. Whilst you must be able to carry out safe and secure deletion of personal data throughout the lifecycle of the device, if you use a mobile device management service (which allows you to track the device in real time), make sure you only use the data the device generates for the specified purpose. This will normally exclude using the data for monitoring purposes.

5. Take all reasonable steps not to access, copy or use any personal content held on the device, except where permitted by the DPA. If inadvertent access/copying takes place, ensure it is remedied swiftly (e.g. data is deleted).
Finally, bear in mind that you may receive a data subject access request, which may require you to examine a BYOD or otherwise confirm such devices do not contain relevant information.

**Identify BYOD usage costs and establish who is going to bear them**

Broadly speaking, BYOD usage costs fall into three categories:

1. Day-to-day running costs, including voice and data charges. Decide in advance whether the employee bears the full cost or whether you will reimburse him/her for a portion of the expense.

2. Technical support, repair and maintenance. Are you willing and able, and does it make business sense, to offer any of these in-house? This option may be cheaper and help maintain confidentiality and data protection compliance.

3. Responsibility for loss of any personal content. If you were to remote wipe a device, the process may lead to loss of personal content, such as downloaded music and videos, personal photographs etc. Are you willing to assume responsibility for the loss? If so, to what extent?

Finally, if any of your employees travel overseas, agree in advance whether you permit roaming, whether you will pay for roaming charges and whether payment will be limited to business use only.

*This briefing has been produced on the author’s laptop whilst accessing her workplace IT system.*

---

**BYOD and roaming charges**

A recent article in the New York Times described the roaming costs challenges faced by Coca-Cola. EU-wide costs were so prohibitive, the company forbade its 2,000 European-based cross-border employees from using even basic device features such as email and Skype. GlaxoSmithKline Biological advised some 13,000 of its employees to avoid using mobile network data when roaming, for the same reason.