Blurring the line between work and play

Firms adopting BYOD need to understand what risks are involved and ensure the content and tone of policies are right

THE CONSUMERISATION OF TECHNOLOGY, fuelled by widespread adoption of smartphones and tablets, has gone a long way towards breaking down the barriers between personal and corporate devices. However, although staff and employers alike may have welcomed the option to bring your own device to work (BYOD), there is growing recognition that the effective implementation of such strategies must also address the wider aspects of employment and data security.

For employees, BYOD increases the opportunity to work flexibly and means only one device may be required for business and personal use. For employers, there may be productivity benefits – with employees carrying work out anywhere and anytime, while lowering costs, as employees use their own devices and, perhaps, even pay for the data used.

However, such arrangements can place stress on an increasingly blurred line between work and home life. Concerns also arise that employers may face heightened risks and challenges, in particular relating to their legal obligations to comply with EU data protection law. For example, specific restrictions apply on transferring personal data outside the EU.

Whether reviewing an existing BYOD regime or contemplating allowing staff to use their personal devices in the workplaces, employers must ensure they understand the risk landscape.

In the UK, the Information Commissioner's Office has published helpful guidance for employers looking to implement BYOD schemes. As UK data protection legislation is intended to implement the Data Protectiion Directive 95/46/EC, much of this guidance will be of relevance to employers across the EU.[1]

Security of data

The starting point for any employer is that it will remain legally responsible for all processing of personal data for which it is the data controller, regardless of this taking place on a BYOD device. Employers cannot delegate responsibility for the security of personal and confidential data. In particular, the Directive requires that organisations take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. The serious loss of personal data by businesses can be very damaging to corporate reputation and, in the UK, can lead to the imposition of a substantial fine, up to £500,000 (€626,700) (or higher for Financial Conduct Authority-regulated businesses).

Employers are advised to approach this area by first auditing the personal data being handled and the devices on which they intend to allow information to be held. This process should include a review of whether information with any particular confidentiality or sensitivity ought to be restricted for use only on corporate systems and devices. A key point to bear in mind is that introducing BYOD should not compromise or introduce weaknesses into existing secure environments for sensitive information.

As part of a BYOD programme, personal data could often be processed in one or a number of locations, depending on the specific strategy adopted. Some of the options may include processing the data on a secure part of the existing corporate IT infrastructure; on the device itself; or within a cloud-based solution. Regardless of where the processing takes place, appropriate measures must be taken to safeguard confidentiality and security and, in particular, to prevent unlawful access if the device is lost or stolen.

Although corporate mobile devices will already have been set up with these issues in mind, it is vital that similar considerations are applied to the use of BYOD. This will include the usual suite of measures, such as data encryption, the use of strong passwords and the automatic locking of devices when inactive. More advanced security measures may be also be required, for example, where the nature of the data or general business pose a greater risk. Numerous options may include measures such as advanced biometric capabilities and multifactor user authentication as these become increasingly available.

Employers should consider the implications of BYOD being used on non-secure networks, such as open Wi-Fi networks or in airports or coffee shops. It may be advisable to require all access to corporate information to be made only through a virtual private network or other secure platform, while prohibiting copying to a non-secure location.

Experience continues to show that education plays a key role in the ongoing management of the BYOD process. Employers must, therefore, take steps to ensure staff understand the importance of maintaining appropriate security and working practices. For example, it may not be appropriate to allow connectivity with other devices using Bluetooth if this could place corporate data at risk. Similarly, employers may wish to place restrictions on the downloading of any personal apps that could pose any security risk to corporate information. Furthermore, employees may also be required to disable any functions or apps that may automatically make backup copies or sync to the cloud or home PCs.

Management and control

A key question for employers is how control over any corporate information that will be held on personal devices owned by employees may be exercised. The employer is responsible for ensuring the confidentiality and security of corporate data on the device and must, therefore, be able to access or delete that data, should the device be lost, stolen, given away, sold, or when the employee leaves the business.

Technology is now widely available that enables such control to be established. Many organisations use third-party mobile device management (MDM) software, which enables devices to be located and offer the option to remotely delete specific data or even wipe the entire device. Where data is stored on the device itself, consideration should be given to segmenting a part of the device, which will enable corporate data to be deleted without affecting an employee's private files.

With employers looking to exercise control over personal devices, conflicting expectations can arise between the parties. In response to employers' taking steps to manage the risks of BYOD, by asserting more robust controls through detailed policies, some employees have raised concerns that such policies may be going too far. Therefore, employers need to ensure they strike the right balance between safeguarding company information and meeting their legal obligations, while ensuring BYOD policies do not affect trust in the relationship, by minimising any effect on personal use and private life.

Take for example the use of MDM solutions, which can enable the location of a device to be tracked in real time. It is easy to see how this may be a useful function for employers and, potentially, a safety and welfare measure. However, any such use ought to be justified by a legitimate business purpose and limited to core business hours. The failure to address this issue could see employers obtaining and processing private information on employees, in breach of EU data protection law, which requires the collection of personal data to be relevant and not excessive. Most importantly, however, could be the effect on staff morale and damage to trust that excessive recording or monitoring could bring about.

A further challenge may arise under BYOD where misconduct is suspected and where corporate data held on the device is considered necessary for an investigation to take place. Although this risk might be less if BYOD allows only secure access on a corporate network, instances could still arise over alleged misuse of the device itself. As such, employers will have to consider building a right into any BYOD policy to inspect and access data on the device, where necessary for a legitimate business purpose.

Striking a balance

To address these risks, employers should carry out an impact assessment, which should consider the business case for monitoring; its effect on privacy; whether the same benefit might be achieved in a less intrusive way; and whether monitoring is justified in the proposed circumstances.

An effective BYOD policy must go beyond the key issues of security requirements, privacy, and monitoring. There are a wide range of other issues that should also be considered, as part of the development or review of an existing BYOD strategy. Some of these issues would address practical matters, such as who is responsible for costs, repair, insurance, data charges and the restrictions, if any, on the use of BYOD roaming calls and data charges. Tax implications may also arise from any benefit an employee derives as a result.

Lessons are being learnt, sometimes the hard way, by organisations allowing the use of personal devices in the workplace. Given the need to strike an appropriate balance between protecting the corporate entity and respecting the privacy of employees, many have found that the tone of the BYOD policy could be as important as the content, for the policy to be effective.

Alan Delaney is an associate in the employment team at Maclay Murray & Spens LLP

[1] The guidance can be found at: http://bit.ly/Z6MjDd

The essentials of a BYOD policy

- What monitoring may take place; explaining when and why for legitimate business purposes
- Scope and purpose of policy – will it apply to employees or also contractors, with modifications and additional protections?
- Security measures the employee is required to take and confidentiality obligations
- Approved devices that can be used
- Steps to be taken if device is suspected as lost or stolen
- Right to withdraw BYOD at any time
- Scope for disciplinary action to be taken for non-compliance
- Corporate ownership of all data created using the device in the normal course of business
- Reimbursement of any costs and any tax implication. Use of BYOD abroad and liability for roaming charges
- Limitations on use, including personal use of device
- Technical support offered, if any
- Appropriate use standards where business systems accessed
- Process to be followed on termination of employment
- Agreement on right to monitor, access and delete information on the device, for legitimate business purposes
- Reassurance as to policy not being used to seek access to private information held outside corporate partition (if relevant)