fairways Est. 1984
hr business support
and recruitment specialists

Head Office:
Balmoral Suite, Royal British House,
Perth, PH2 8HA
Phone: +44(0)1738 632 561

Dundee Office:
Exchange Court, Exchange Street,
Dundee, DD1 3DE
Phone: +44 (0)1382 211 222

HR Guidance

Bring your own device (BYOD)

This business guide highlights the potential risks and benefits for businesses of allowing employees to use their own personal mobile devices (such as tablets, smartphones, laptops or notebook computers) for business purposes.

Bring your own device (BYOD)

Fairways HR guidance only provides an overview of the law in this area. For a complete understanding of how it may affect your particular circumstances in the workplace please contact one of our Consultants.

What is bring your own device (BYOD)?

Many employees now own personal mobile devices (such as tablets, smartphones, laptops or notebook computers) that can be used for business purposes. Businesses are receiving an increasing number of requests to allow employees to use these devices at work.

BYOD benefits

BYOD can bring a number of benefits to businesses, including:

- Increased flexibility and efficiency in working practices.
- Improved employee morale and job satisfaction.
- A reduction in business costs as employees invest in their own devices.

BYOD risks

The boom in BYOD has been matched with an upsurge in activity by criminals trying to exploit the data and intellectual property stored on personal mobile devices. The use of personal mobile devices for business purposes increases the risk of damage to a business's:

- IT resources and communications systems.
- Confidential and proprietary information.
- Corporate reputation.

Ownership of the device

Personal mobile devices are owned, maintained and supported by the user, rather than the business. This means that a business will have significantly less control over the device than it would normally have over a traditional corporately owned and provided device.

BYOD risks (continued)

Securing data stored on the device

- A business is responsible for protecting company data stored on personal mobile devices. Businesses should consider implementing security measures to prevent unauthorised or unlawful access to the business's systems or company data, for example:
  - Requiring the use of a strong password to secure the device.
  - Using encryption to store data on the device securely.
  - Ensuring that access to the device is locked or data automatically deleted if an incorrect password is inputted too many times.
- The business should ensure that its employees understand what type of data can be stored on a personal device and which type of data cannot.

Mobile Device Management

Mobile Device Management software allows a business to remotely manage and configure many aspects of personal mobile devices. Typical features include:

- Automatically locking the device after a period of inactivity.
- Executing a remote wipe of the device (make sure employees are aware which data might be automatically or remotely deleted and in which circumstances).
- Preventing the installation of unapproved apps.

Monitoring use of the device

- If a business wants to monitor employees' use of personal mobile devices, it must:
  - make its reasons for monitoring clear; and
  - explain the benefits the business expects will be delivered by monitoring (for example, preventing misuse of the device).
- The business must ensure that monitoring technology remains proportionate and not excessive, especially during periods of personal use (for example, evenings and weekends).

BYOD risks (continued)

Loss or theft of the device

- The biggest cause of data loss is still the physical loss of a personal mobile device (for example, through theft or by being left on public transport).
- Loss or theft of the device could lead to unauthorised or unlawful access to the business's systems or company data. The business must ensure a process is in place for quickly and effectively revoking access to a device in the event that it is reported lost or stolen.
- Businesses should consider registering devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft.

Transferring data

- BYOD arrangements generally involve the transfer of data between the personal mobile device and the business' systems. This process can present risks, especially where it involves a large volume of sensitive information. Transferring the data via an encrypted channel offers the maximum protection.
- Employees should be encouraged to avoid using public cloud-based sharing which have not been fully assessed. Businesses should consider providing guidance to employees on how to assess the security of wi-fi networks (such as those in hotels or cafes).

Departing employees

A business needs to think about how it will manage data held on an employee's personal mobile device should the employee leave the business.