Black Graf solicitors LLP

Bring your own Device (BYOD)

This newsletter highlights the potential risks and benefits for businesses of allowing employees to use their own personal devices (such as laptops and smartphones) for business purposes. Businesses are receiving an increasing number of requests to allow employees to use personal mobile 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 by 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':

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

Ownership of the device?

As the device is owned, maintained and supported by the employee, rather than the business, the business will have significantly less control over the device than it would normally have over a traditional corporately owned and provided device.

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' 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 access to the device is locked or data automatically deleted if an incorrect password is inputted too many times.

A business should ensure its employees understand which type of data can

If you would like to discuss any of the matters raised in this newsletter please contact:

Jane McKee
jmk@blackgraf.com

Tel: 020 7586 1141

The information in this newsletter is not meant as a substitute for advice on particular issues and is written in general terms. You should seek specific advice before taking any action based on the information in this newsletter.

Black Graf LLP 100 Baker Street London W1U 6WG
Black Graf LLP is a Limited Liability Partnership registered in England and Wales registration no: OC334046. Any reference to a partner is to a member of Black Graf LLP. Authorised and regulated by the Solicitors Regulation Authority no: 488394
www.blackgraf.com

This newsletter outlines the law as it stands at the date of writing in December 2014.

be stored on a personal device and which type of data cannot.

Mobile device management?

Mobile Device Management software allows a business to remotely monitor 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 the use of data?

If a business wants to monitor employees' use of a personal mobile device, it must:

- Make its reasons for doing so clear; and
- Explain the benefits the business expects will be delivered by monitoring.

Monitoring must remain proportionate and not excessive, especially during periods of personal use (e.g. weekends).

Loss or theft of the device?

The biggest cause of data loss is the loss of the mobile device (for example, through theft).

The business must ensure a process is in place for quickly and effectively revoking access to a device in the event it is reported lost or stolen. Businesses should consider registering a device with a remote locate and wipe facility to maintain confidentiality of the data in the event of loss or theft.

Transferring data?

BYOD arrangement generally involve the transfer of data between the business' systems and the personal mobile device. This process can present risks, especially where it involves a large volume of sensitive information. Transferring data via an encrypted channel offers the maximum protection.

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.