SME Business Guidance Series

Bring Your Own Device (BYOD)

Provided by:

Crendon Insurance Brokers

www.crendoninsurance.co.uk
enquiries@crendoninsurance.co.uk

11 Greenfield Crescent, Edgbaston, Birmingham B15 3AU
Tel: 0121 45 45 100

Personal devices, such as smart phones, tablets and laptops, have risen in popularity throughout the United Kingdom due to technological advancements and wider availability. As a result, more people are now also using their personal devices to conduct work activities, a trend called 'Bring Your Own Device' (BYOD). A recent study by YouGov revealed that 47 per cent of all UK adults now use personal devices for work purposes. However, many businesses still have an indifferent attitude concerning use of personal devices for work business, which can place personal and sensitive data protected under the Data Protection Act 1998 (DPA) at risk.

The following guidance provides an overview of the risks your business faces concerning personal devices and what to consider when deciding whether to offer a BYOD policy to your employees.

Understanding the Risks and Benefits of BYOD

Employers and other data controllers are responsible for following the DPA principles and protecting any personal and sensitive data under their control, regardless of who owns the device that is processing data. This means that if you allow employees to use their own personal devices to access and store business data, you must have appropriate security measures in place to prevent data from being accidentally or deliberately compromised.

Assessing the Risks

The main risk concerning BYOD is data security. Because employees own, maintain and support the devices, the employer will have significantly less control over the devices compared to traditional corporate-owned devices. Employees may accidently download malware or allow family members and friends access to confidential information on their personal devices without the employer even knowing. Coupled with the lack of control is the fact that there may also be a large number of devices as well as different types and brands of personal devices, making data security more difficult for the IT department.

While data security is the primary concern, you will still need to make sure that your BYOD policy is compliant with all other aspects of the DPA. BYOD policies could raise the risks of personal data being processed for a different purpose from what it was originally collected for, accidental data leakage without the user's knowledge and data becoming out of date or inaccurate over time.

What are the Benefits?

An effective BYOD device policy can benefit your business in many ways. It can reduce upfront hardware costs and lead to improved employee satisfaction, overall morale increase, increased job efficiency and increased flexibility for your employees. When creating procedures to mitigate your BYOD data risks, you also have the opportunity to review your current data protection standards and implement any changes to make them even stronger.

Considerations for Creating a BYOD Policy

Every business will have its own needs to address in a BYOD policy. It is important to make sure that all users connecting their own personal devices to your IT systems are fully trained on the policy and aware of their responsibilities. Make sure to address following areas when implementing your policy.

What Type of Data is Held?

Your starting point should be conducting an internal audit of the different types of personal data you are or will be processing and the devices to be used, including their ownership. You need to decide which types of data can be processed on a personal device and which must be held in a more restrictive environment. You also need to consider the fact that employees' personal devices will contain their own personal, non-corporate information about them and others that use the devices, including family members. Will you end up processing any of that sensitive personal data as well, and if so, are there controls in place?

Where is the Personal Data Stored? How is it Secured?

Typically, personal data being processed on a personal device is stored in one or more of the following locations:

- On the device itself
- On a service within the organisation's IT network
- In a private, community or public cloud

Regardless of where your data is stored, you will need to take appropriate measures to protect against unauthorised or unlawful access, including access to lost or stolen devices. Appropriate measures can include:

- Creating an Acceptable Use Policy to provide guidance and accountability
- Controlling access to the data or device by using a password or PIN
    - Make sure that the password is strong and changed regularly.
    - Automatically lock the device if it is inactive for a period of time or if an incorrect password is entered too many times.
    - If data is stored in a remote location, such as a corporate network or cloud, consider additional access credentials.
- Creating a plan of action in case a device is lost or stolen
    - This plan should quickly and effectively revoke access to a device.
    - Equip devices with a Sat Nav locator and remote wipe capability.
- Encrypting the data
- Identifying types of storage media on the device, including micro or mini SD cards
    - Because most types of storage media are easily removable, a loss or theft of data can go unnoticed for a long period of time.
- Restricting data to be contained within specific apps or programs
    - You can also restrict access and require additional authentication to certain apps or data based on geographic location.
- Ensuring the safe and secure deletion of data throughout the device's life cycle, including if it gets sold or transferred to a third party

How is the Data Transferred?

BYOD arrangements can involve the transfer of large amounts of data between a personal device and the business's network system. Data in transit can be subject to attacks during the transfer process. Review all channels in which data may be transferred, including email, removable media and public cloud services. Consider taking the following actions:

- Transferring personal data through an encrypted channel, such as a VPN or HTTPS
- Monitoring data transferred for data leakage or loss
    - You need to be aware of privacy concerns when monitoring during periods of private use.
- Disabling some interfaces that might be used to connect to other devices
- Providing guidance to employees on how to assess the security of available Wi-Fi networks

How will the Device be Controlled?

Because businesses have relatively little control over the personal device in BYOD policies, you need to plan in advance how to ensure the confidentiality of any stored personal or sensitive data. Create a plan of action for when an employee using BYOD leaves employment. You also want to make sure that apps and software downloaded onto the device are secure and not harmful. This can be accomplished by:

- Ensuring that the operating system and other software are appropriately patched or updated
- Determining who can install third-party programs and where programs can be downloaded from
- Providing guidance to users about the risks of downloading untrusted or unverified apps
- Maintaining a clear separation of personal data processed on behalf of the business and data processed for the device owner's own purposes
    - Use different apps for business and personal use.

Monitoring at Work

When an employee uses a personal device, at least some of the use will be personal in nature, especially during certain times of the day, such as evenings and weekends. Employees have a legitimate expectation of keeping their personal lives private, and are entitled to a certain degree of privacy in the work environment. If you wish to monitor your employees, you need to be clear about the purpose of the monitoring and show that your particular monitoring arrangements are justified by real benefits.

By assessing your risks and implementing strong security measures to comply with the DPA, a BYOD policy may be a great benefit to your business. Regularly review your BYOD policy to ensure DPA compliance and that the most up-to-date security measures have been implemented to protect personal and sensitive data.