

Smart Phone Policy - BYOD

Template v1.1 – Updated September 2023

This is a template policy which can be downloaded and adapted by an organisation letting staff use their own devices for work.

Some organisations allow staff to use their own smart phone for work purposes rather than supply them with a separate work-only device. Such an approach has been termed BYOD or 'Bring Your Own Device'. While there can be advantages to this, such an approach can put the organisations data and reputation at risk unless those devices are correctly managed. Therefore, it is not recommended for an organisation to adopt a BYOD approach without having a Mobile Device Management (MDM) solution. You can find out more about MDM’s on the [Digitising Social Care website](http://www.digitisingsocialcare.co.uk/get-help-set-and-use-technology/keeping-mobile-and-tablet-devices-secure).

The exact wording of this policy will depend on the MDM solution used by your organisation - for example the manner in which devices will be enrolled. However, this template should provide a good starting point for developing an individual organisation's own specific policy.

# Use of Smart Phones at Work Policy

Introduction

This Bring Your Own Device Policy is *insert organisation name here’s* (hereafter referred to as "us", "we", or "our") policy regarding the safe use of personal smart phones used by our staff for work-related purposes.

Modern smart phones are capable of accessing and storing data, and running business applications. While the use of smart phones can bring many benefits, and help staff to better do their jobs, it also introduces a significant risk. That risk is that data, or access to that data, may fall into the wrong hands due to the loss or improper use of a smart phone.

  As an organisation we have taken a decision to allow staff to use their own smart phone for work purposes. This policy has been developed to ensure that this organisation's data is not put at risk from the use of smart phones in this manner. For those members of staff with a business requirement to access the organisation’s data with a smart phone, this policy provides the necessary guidance so that it is done in a manner that does introduce unacceptable threats to the safety and integrity of this data.

Purpose

The purpose of this policy is to:

Provide effective controls to ensure that staff access to our data and any information systems through the use of a smartphone is authorised, secure and confidential, in line with our business requirements

Ensure the remote processing of our data is operated in accordance with statutory requirements and all relevant guidance

Ensure that any risks associated with smart phone based access are recognised, assessed and managed.

Scope

This policy applies to allstaff.

Definitions

Personal Data:Information that relates to an identified or identifiable individual, as defined by the Data Protection Act 2018 and the GDPR.

Smart Phones: A mobile phone that allows users to store information, use email and install programs.

User: Any person authorised to access *organisation name's* IT systems and networks remotely.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing the key. The result of the process is encrypted information. Password protection is not a form of encryption.

Bring Your Own Device (BYOD):The term used to describe the approach of letting members of staff use their own mobile device for work purposes. For example, an organisation might allow their staff to use their own smart phones to access work e-mail while out of the office, rather than supplying corporate owned devices for that specific task.

Mobile Device Management (MDM) Service: A service that allows an organisation to remotely control, monitor and enforce policies on employee mobile devices. This lets an organisation ensure that the devices meet required compliance to protect any data that may be processed by or stored on the device.

Smart Phone Access Authorisation

We note that not all organisations will use a MDM. If you have chosen not to request that staff use a MDM to access data on their personal phone, you should outline the security processes you have put in place to protect your data in this section.

For a member of staff to obtain authorised and secure smart phone access to our data and be issued with the required instructions for enrolling into our MDM, *insert appropriate job role here* should ensure the user complete a New 'Smart Phone Access' registration form.

Having obtained the required authorisation, a user must enrol their smart phone in our MDM before they can access any of our data or use their phone for work purposes.

*(The exact nature of this enrolment would depend on the MDM used by the organisation. This might take the form of:*

* *Accessing a specific URL to initiate the enrolment process*
* *Automatic registration the first time the user attempts to access data (e.g. email)*
* *A manual process by which the user brings their phone into the office and has it enrolled by the IT department.)*

If the phone does not meet required specifications for enrolment or the user does not agree for it to be managed, or with any of the policies to be applied, then the phone will not be enrolled into the MDM and will not gain access to any data or services.

Technical problems or queries regarding remote access or mobile devices should be addressed to *insert appropriate job role here*.

 Authorised Users and Smart Phones

We maintain a log of all users who are authorised to access our data on their personal phones. This log is available *insert location here.*

All authorised users will have enrolled their designated smart phone with the MDM service before attempting to access *organisation name's* data or services

Users must inform their Line Manager when access is no longer required, or when leaving the organisation. All *organisation name's* data and apps will be deleted from the user's smart phone before it is unenrolled from the MDM service*. (In the case an MDM is not used, all data belonging to the organisation will be removed from the device as part of the leaver’s process.)*

User Responsibilities for the Security of Smart Phones

Users must not deliberately put their authorised smart phone at undue risk of being stolen, lost or accessed by unauthorised persons.

Stolen or lost equipment must be reported as soon as possible to *insert role responsible here.*

Users will not use personal smart phones to access *organisation name's* services or data unless that smart phone has been authorised for such access as part of the BYOD scheme, and has been enrolled in the MDM service

Users will not store any personal confidential data on personal smart phones unless that smart phone has been authorised to store such data as part of the BYOD scheme, and has been enrolled in the *organisation name's* MDM service

Users will not attempt to connect to *organisation name’s* corporate wireless network with personal smart phones unless that smart phone has been authorised for such access as part of the BYOD scheme, and has been enrolled in the *organisation name's* MDM service.

 Where available users may connect their personal smart phone to the organisation's guest wireless network to get internet access.

User Responsibility for the Security of Personal Confidential Data and Information

*Organisation name's* data should only be remotely accessed, held and processed on smart phones authorised and enrolled in ourMDM service.

Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems via the user's enrolled smart phone. Smart phone screens should be locked when not actively being used.

The use of smart phones for accessing ourdata or services in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of an unlocked device.

Data should not be held on a smart phone for longer than it is required and should be deleted or archived promptly to reduce the risk of the data being accessed by the wrong person.

Personal confidential data must not be stored on an unencrypted device(NB: Password protection is not a method of encryption and must not be relied upon as such).

Emails containing personal confidential data and other confidential information must not be sent to or from personal email accounts.

Reporting Security Incidents and Weaknesses

Staff are responsible for smart phones and all data held on them. In the event of loss, theft or any data security incidents associated with smart phone use, users must inform *insert job role here* and follow the data breach procedures in our Data Security Policy.

Duties and Responsibilities

You should update the responsibilities below based on what makes sense for your organisation, the following are suggestions, you do not need to have someone in each of these roles if it does not make sense for your organisation.

Chief Executive Officer

The Chief Executive is responsible for ensuring that the organisation complies with the statutory and good practice requirements governing smart phone use outlined in this policy and is supported by the delegated management responsibilities outlined below.

All Managers

All Managers as Information Asset Owners are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance

Senior Information Risk Owner (SIRO)

The SIRO has executive lead responsibility for Information Risk and providing high level assurance to the senior leadership team. At Organisation name’s SIRO is the*fill in responsibilities as appropriate.*

All Staff

All staff must ensure that they are aware of their responsibilities for complying with smart phone use requirements in accordance with this policy. All staff with authorised smart phones must safeguard our information and report immediately any associated security incidents.

 Staff Training

It is mandatory for all new staff to undertake the *insert name*training relevant to their post as part of their induction process. It is mandatory for all staff to complete the refresher training every twelve months.

Staff must inform *insert appropriate job role here* if they do not understand any aspects of this policy and/or require further associated training.

Any specific training needs identified to ensure compliance with this policy should be referred to *insert appropriate job role here*.

 Monitoring and Review

Add a statement about how you will monitor and review this policy

Approval

This policy has been approved by the undersigned and will be reviewed at least annually.

|  |  |
| --- | --- |
| Name |  |
| Signature |  |
| Approval Date |  |
| Review Date |  |