

Smart Phone Policy for Organisation Supplied Devices

Template – Version 1

**This is a template that could be used by an organisation providing smart phones for their staff. This policy does not explicitly mentiona Mobile Device Management (MDM) solution.This is because the smart phones are being provided by the organisation. If, as would be recommended, the organisation is using an MDM solution then the supplied smart phone will already have been enrolled before the end user receives it. However, the policy is still relevant for an organisation that is not using an MDM but is just supplying adequately protected smart phones that are preconfigured before distribution.**

**You can find out more about MDMs on the** [**Digitising Social Care website**](http://www.digitisingsocialcare.co.uk/get-help-set-and-use-technology/keeping-mobile-and-tablet-devices-secure)**.**

# Introduction

* 1. This Smart Phone Policy ***insert organisation name here’s*** (hereafter referred to as "us", "we", or "our") policy regarding the safe use of smart phones which we supply to our staff.
	2. 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.
	3. This policy has been developed to ensure that this organisation’s data is not put at risk from the use of smart phones. 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 not introduce unacceptable threats to the safety and integrity of this data.

# Purpose

The purpose of this policy is to:

* 1. Provide effective controls to ensure that our Staff’s access to our data and any information systems using a smart phone is authorised, secure and confidential, in line with the organisation’s business requirements
	2. Ensure the remote processing of our data is operated in accordance with statutory requirements and all relevant guidance
	3. Ensure that any risks associated with smart phone-based access are recognised, assessed and managed.

# Scope

* 1. This policy applies to all staff who have been issued with a smart phone. A list of staff who have been given access to a smart phone is available in our Information Asset Register

#  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 member of staff who has been issued with a smart phone and authorised to access our 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.

# Smart Phone Access Authorisation

* 1. For a member of staff to obtain authorised and secure smart phone access to our data and be issued with the required mobile device, their relevant Line Manager should ensure the user complete a mobile device assignment form.
	2. The type of smart phone available for use will be decided by **insert name of individual responsible for this here.**
	3. Managers should not just transfer phones from one staff to another but undertake the correct process to re issue a phone to a new user. **You should include your processes here. This might include factory resetting the phone.**
	4. Technical problems or queries regarding remote access or mobile devices should be addressed **to insert name of individual responsible for this here.**

# Authorised Smart Phones

* 1. We maintain a log of all smart phones issued in our Information Asset Register.
	2. All smart phones issued will be installed with appropriate and approved encryption & PIN control.
	3. Users must return all smart phones to insert the role responsible here. This might be the relevant department or a Line Manager when access is no longer required, or when leaving the organisation. All data from returned devices should be deleted or archived and the device reset and wiped.

# User Responsibility for the Security of Personal Confidential Data and Information

**Note that you may wish to alter these based on your own organisation’s policies.**

* 1. All smart phones should be held and transported securely, should not be left unattended (e.g. in vehicles), and should be locked away when not in use.
	2. Stolen or lost equipment must be reported as soon as possible to insert role responsible here.
	3. Users must not install any unauthorised or unlicensed software on any organisation name's issued smart phone
	4. Issued smart phones should not be used for non-business-related purposes.
	5. Issued smart phones must only be used by the individual that they have been issued to. A user may not share the device with or lend it to anyone else, for example a family member or work colleague.

# User Responsibility for the Security of Personal Confidential Data and Information

* 1. Our data should only be remotely accessed, held and processed on smart phones supplied or authorised by **Organisation name’s**.
	2. Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems. Smart phones should not be shared with any other person, even for temporary access to a non-work related app or service. Smart phone screens should be locked when not actively being used.
	3. The use of smart phones in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of equipment.
	4. Staff must ensure that Organisation name’s smart phones and information accessed at home are secure from theft and damage and cannot be accessed by family members, friends or any other unauthorised user.
	5. 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.
	6. 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).
	7. Emails containing personal confidential data and other confidential information must not be sent to or from personal email accounts.

# User responsibility for the use of Personal Smart Phones

* 1. Users will not use personal smart phones to access our services or data.
	2. User's will not store any personal confidential data on personal smart phones.
	3. User will not attempt to connect to the organisation's corporate wireless network with personal smart phones.
	4. Where available, users may connect their personal smart phone to the organisation's guest wireless network to get internet access.

# Reporting Security Incidents and Weaknesses

* 1. 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

* 1. **Chief Executive Officer (or equivalent job role)**
	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.
	2. **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
	3. **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.***
	4. **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 and supporting guidance.

All staff with authorised smart phones must safeguard equipment and information and report immediately any associated security incidents.

# Staff Training

* 1. It is mandatory for all new staff to undertake ***insert name of training here*** training relevant to their post as part of their induction process. It is mandatory for all staff to complete refresher training every twelve months.
	2. Staff must inform **insert appropriate job role here** if they do not understand any aspects of this policy and/or require further associated training.
	3. 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

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

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