# Use of Smart Phones at Work Policy

## Use of Smart Phones at Work Policy

### 1. Introduction

1.1. This Bring Your Own Device Policy is *Cedar Lodge Care Home'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.

1.2. 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.

1.3. 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.

### 2. Purpose

The purpose of this policy is to:

2.1. 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

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

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

### 3. Scope

3.1. This policy applies to all staff

### 4. 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 *Cedar Lodge Care Home'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.

## 5. Authorised Users and Smart Phones

5.1. We maintain a log of all users who are authorised to access our data on their personal phones. This log is available in Cedar Lodge's Manager Office.

5.2. Users must inform their Line Manager when access is no longer required, or when leaving the organisation. All data belonging to the Cedar Lodge will be removed from the device as part of the leaver's process.

## 6. User Responsibilities for the Security of Smart Phones

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

6.2. Stolen or lost equipment must be reported as soon as possible to *the Care Home's Manager.*

6.3. Users will not use personal smart phones to access *Cedar Lodge Care Home's* services or data unless that smart phone has been authorised for such access as part of the BYOD scheme.

6.4. 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.

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

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

7.1. *Cedar Lodge Care Home's* data should only be remotely accessed, held and processed on authorised smart phones.

7.2. 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.

7.3. The use of smart phones for accessing our data 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.

7.4. 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.

7.5. 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).*

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

## 8. Reporting Security Incidents and Weaknesses

8.1. 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 *the Data Protection Champion James Hunt* and follow the data breach procedures in our Data Security Policy.

## 9. Duties and Responsibilities

### *9.1. 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

### *9.2. 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.

## 10. Staff Training

10.1. It is mandatory for all new staff to undertake the *Data Security Awareness* 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.

10.2. Staff must inform *the Data Protection Champion, James Hunt,* if they do not understand any aspects of this policy and/or require further associated training.

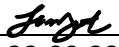
10.3. Any specific training needs identified to ensure compliance with this policy should be referred to *the Data Protection Champion*.

## 11. Monitoring and Review

This policy will be monitored and updated as necessary.

## 12. Approval

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

| | |
|---|---|
| Name | James Hunt |
| Signature |  |
| Approval Date | 22.09.23 |
| Review Date | 29.06.23 |