Mobile Phone Guidelines

Aim

The SOS Homecare Ltd mobile phone policy offers general guidelines for using personal and company mobile phones during work hours.

The purpose of this policy is to help us all get the most out of the advantages mobile phones offer our company while minimising distractions, accidents, and frustrations improper mobile phone use can cause.

As an organisation we have taken a decision to allow staff, in certain circumstances, 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 not introduce unacceptable threats to the safety and integrity of this data.

This policy applies to all SOS Homecare Ltd employees.

Policy

The following are SOS Homecare Ltd basic guidelines for proper employee mobile phone use during work hours. In general, mobile phones should not be used when they could pose a security or safety risk, or when they distract from work tasks:

- Never use a mobile phone while driving.
- Never use a mobile phone while operating equipment.
- Do not use mobile phones for surfing the internet or gaming during work hours.
- Avoid using work mobile phones for personal tasks.
- Avoid using personal mobile phones for work tasks.
- Do not use mobile phones during meetings.
- Do not use personal mobile phones to record confidential information.
- Do not call premium rate numbers on a work phone unless authorised by your Line Manager
- Work phone data is not to be used other than emails, CarePlanner website and the use of PASS app
- Do not lend a company mobile phone to any other staff member.
- Never take photos inside a client's house, with the exception of receipts being uploaded onto the PASS app

We realise the mobile phones can be great tools for our employees. We insist that if you have been given a work mobile phone, that this is used. We encourage employees to use mobile phones:

- For making or receiving work calls in the appropriate place and situation to do so.
- For other work-related communication, such as text messaging or emailing in appropriate places and situations.
- To schedule and keep track of appointments.
- To carry out work-related research.

- To keep track of work tasks.
- To keep track of work contacts.

All employees that are required to use their smart phone for work should not;

- Take screenshots of any of the documents
- Download the documents and save them onto their device
- Allow anyone other than themselves to view the application or work-related data
- Access the data once their employment has ceased
- Access data when they are not in work

If you have any technical problems or queries regarding remote access or mobile devices, these should be addressed to your line manager.

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 your Line Manager.

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.

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

All devices should be locked with a password or pin, any log in information should not be stored or saved within the device, new credentials should be inputted every time.

Improper use of mobile phones may result in disciplinary action.

Reporting Security Incidents

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 Line Managers immediately and follow the data breach procedures within Confidentiality, Data Protection and GDPR policy.

Review

This policy is to be reviewed every 2 years.