STAIRLOCK

MOBILE PHONE & ELECTRONIC DEVICES POLICY

Stair Lock provides this policy to set out guidance relating to use of mobile phones by employees.

Inappropriate use of mobile phones at work decreases productivity, causes security risks, distracts co-workers and colleagues, and can create significant safety risks. This policy outlines minimum standards regarding telephone/mobile, electronic device such as tablets, and headphone use for all employees during their employment.

Stair Lock understands that staff may have a need to make and receive personal telephone calls or messages during work hours. However, mobile phone use should never interfere with employees' work duties. When working in high-risk environments such as building sites, the factory or warehouses, it is important that you are alert and aware of your surroundings at all times to prevent accidents or injuries to yourself or others.

The following guidelines govern the use of mobile phones while at work:

- Personal calls, messages or use of mobiles should not take precedence over the service of customers, except in the case of emergency.
- Anyone working in a high-risk environment such as the factory or warehouse must be alert at all times, and therefore it is not permitted to use a mobile phone while inside the high-risk area (regardless of whether it is a Stair Lock or personal phone and regardless of purpose). The only exception to this is when use of the device is required to carry out duties, such as troubleshooting machinery issues with a technician over the phone. During these instances, the user is to take due care in ensuring their safety and the safety of others.
- When inside the factory or warehouse, mobiles are only permitted to be used in separate office areas or during breaks in lunchrooms or in outside rest areas. When not on break or in the permitted area, mobiles must be stored in an appropriate area (e.g. locker, car, etc) unless approved by your supervisor to be kept elsewhere.
- If you require your device to be on your person whilst in a high risk area you must seek approval from your supervisor, and you must leave the high-risk area before using the device. You supervisor can refuse to grant approval for devices to be on your person during work hours.
- Company mobile phones issued for the purpose of taking work related images are permitted if required to complete your work (such as taking images of products for quality control purposes in the factory), however cannot be used for other purposes such as phone calls, messaging or any other purpose.
- Any employee issued with a Stair Lock mobile phone is also required to adhere to the policy requirements as set out below.
- The above standards also apply to other electronic devices, such as headphones, iPads/tablets.
- Headphones or any other earpiece device is not permitted or to be used in high risk areas during work hours.

Stair Lock Issued Mobile Phones:
Stair Lock provides mobile phones to support the work and accessibility of its management, sales and service staff. The purpose of the policy is to ensure clear understanding of the responsibilities of users and management and to provide guidelines for the acceptable usage of Stair Lock mobile telephones and/or mobile telephone accounts.

1. Mobile telephones are issued on the basis that a user agrees to abide by the company's terms and conditions for acceptable use of Mobile Telephones as detailed in this policy. The company treats misuse of its IT facilities seriously: references to usage include all calls, messages, data transfers and downloads and any other services that are attributable to or associated with a mobile telephone.
2. All users must accept full responsibility for using their company mobile telephone in an honest, ethical, safe and legal manner and with regard to the rights and sensitivities of other people. Use must be in accordance with this policy and all relevant federal and state legislation. Such legislation shall include, but not be limited to legislation covering privacy, copyright, freedom of information, equal employment opportunity, intellectual property and occupational health and safety.
3. The driver of a vehicle must not use a hand-held mobile phone while the vehicle is moving, or while it is stationary but not parked.
4. All devices must only have apps required for business purposes, no personal apps are permitted on work devices.
5. Users should make every reasonable effort to ensure that their mobile telephone is kept charged and switched on when required to perform work duties and furthermore must ensure they use all means available to secure their phones, including but not limited to using a PIN number and recording the IMEI number (*#06#).
6. Users must take due care when using company mobile telephones and take reasonable steps to ensure that the equipment is not damaged or stolen. Users must immediately report any such incidents to the HR Department and must not use equipment if they have reason to believe it is dangerous to themselves or others. Redundant handsets or peripherals must be returned to Head Office. Appropriate covers are provided with every phone and users are required to use them without exception: broken screens and/or iPhone repairs caused by not having the appropriate cover fitted will be at the cost of the user.
7. All users must ensure that the phone is immediately set up with a professional voicemail message, that business related calls and messages are answered/returned promptly and in a professional manner fit to represent the company at all times.
8. When on leave users must ensure that all business calls are actioned during their absence by using one the following methods: setting up a diversion, amending their voicemail advising callers of the leave and alternate number to call, passing on any messages received.

9. While overseas for business purposes, email or text messaging is recommended for non-urgent matters due to excessive international roaming costs of mobile telephone use.

Acceptable / Permitted use of mobile phones:

1. Business related calls, data & SMS
2. Reasonable Personal usage – refer to Carrier specific rules
3. Diversion to landlines or another mobile for taking of leave
4. Data usage due to accessing Business Portal and business emails
5. Emergency calls: 000 or alternatively 112 (which may reach emergency services via an alternative service provider if one is available – also can be dialled anywhere in the world and is automatically translated to the emergency number for that country)

Unacceptable use of mobile phones:

1. The company mobile must not be used for transmission, retransmission, or storing of any unlawful, obscene, indecent, profane, libellous, offensive, pornographic, threatening, abusive, defamatory, or otherwise objectionable information. Without limitation this includes any transmissions constituting or encouraging conduct that would constitute a criminal offence, give rise to civil liability, or violate any law.
2. Any action on a mobile telephone is not allowed that restricts or inhibits the use of Company telephone services or generates excessive telephony traffic through the use of automated or manual programs, routines and downloads.
3. Users shall not cause, or attempt to cause, security breaches or disruptions to telephone communications. Examples of security breaches include, but are not limited to, accessing calls of which the customer is not an intended recipient or logging into a server or account using mobile telephony services that the user is not expressly authorised to access.
4. Harassment is not permitted, whether through language, images, or frequency and size of telephone, text or multimedia messaging calls. Users must not send unsolicited text messages, including “junk mail” or other advertising material.
5. Users must not call premium information: 123, 19, international, competition and entertainment numbers, sign up to non-business related automated services and downloads that may incur additional costs – these costs will need to be reimbursed by the user.
6. Mobile telephones hold and provide access to a range of data sources. The following requirements must be met when storing or accessing data using a mobile telephone:
7. A user must not examine, disclose, copy, rename, delete or modify data without the express or implied permission of its owner. This includes data on storage devices and data in transit through a network.
8. A user must respect the privacy and confidentiality of data stored or transmitted on the Company’s IT facilities. Any release of data to an unauthorised person is expressly forbidden; and
9. Users storing data of a sensitive nature, such as information on individuals must ensure that the privacy of such information is unable to be compromised. In these cases access controls should be employed such as password locks or similar tools.

Access to account information

1. The company has the right to capture and inspect any information made on a company phone or device to:
2. investigate system problems and/or potential security violations
3. maintain system security and integrity
4. prevent, detect or minimise unacceptable behaviour
5. review expenditure charged to a mobile telephone account

Variations

Stair Lock reserves the right to vary, replace or terminate this policy from time to time.

A breach of this Mobile Phone Policy by any employee will result in disciplinary action being taken which may include termination of employment.

Approved by:	*Edward Lloyd*	*Managing Director*	*01 August 2023*