



Mobile Phone Policy

This policy applies to all companies within the Relyon Group.

This policy is designed to clarify the correct and acceptable use of mobile phones for business purposes.

Criteria for Allocation

The allocation of a mobile phone must be approved by a senior manager in circumstances where there is an adequate need or benefit to the company. These circumstances may include;

- The requirement for an employee to undertake frequent out of office duties, including meetings or travel.
- When an employee is on call or standby (phone may be given on a shared basis)
- In relation to a function or role, e.g. security supervisor or building manager
- For greater efficiency and enhance client service

Use of own phone for company

Employees who are not allocated mobile phones but use their own phones for business related call may be entitled to a level of reimbursement from the company.

Employees are required to present their monthly itemised bill with the relevant calls highlighted for reimbursement. An expense claim should be completed for this purpose.

Responsible Use and Security

The appropriate use of mobile phones could lead to theft and/or disclosure of private or confidential information. The phones must only be used by the assigned employee or department and must ensure that usage is lawful and ethical.

Employees who are allocated mobile phones are reminded that the phone is the property of the company and ultimate liability for misuse rests with the user and the company.

Employees should not access, store or distribute any offensive or inappropriate material on mobile devices.

Employees are not permitted to stream music or video content on company mobile phones.

Employees are not permitted to download and games or applications that are not business related.

Reasonable care must be taken to prevent accidental damage, loss or theft of mobile phone equipment. In the event of the theft or loss of a mobile phone, the user must immediately contact their manager or the Control Room if out of hours.

Employees are not permitted to allow non Relyon people to use their devices at any time.

Physical security for the device is the users responsibility and care should be taken not to leave the device unlocked, unattended or visible in an unsecure place.

Where mobile phones are issued to an individual and not a shared device, employees should personalise and activate the messaging service, using the standard script as laid out in the company Employee Handbook and the IT and Telephony Company Standards Procedure.

Storage and protection settings such as PIN numbers are applied to mobile phones. Please ensure these facilities are used at all times.

Excessive Use

All mobile devices are allocated against a usage plan suitable for the nature of the role and have ample allowances for calls and data usage required for the role to be undertaken effectively. Any usage by employees that results in additional use charges exceeding £50 per month will be subject to investigation and may lead to disciplinary action. Should the employee be found to be in breach of this policy, the Company reserves the right to reclaim these costs in line with the terms and conditions laid out in contracts of employment.

Use Whilst Driving

Extreme care should be exercised when using mobile phones in cars. Under Section 3 of the Road Traffic Act 2006, mobile phones can only be used when connected to handsfree units.

It is an offence to drive a vehicle while holding a mobile phone, regardless of whether the phone is being used or even switched on. Any employee who commits an offence under this legislation will be liable for any costs incurred.

Personal Use

From time to time, short and urgent personal calls may be made whilst at work. This privilege should not be abused or the use of the mobile phone may be restricted or removed.

Absence/Leave

Employees may be required to return their mobile phone for certain absences, e.g. long term sick leave and maternity leave. The phone may be temporarily reallocated to other employees to cover this absence/leave.

Monitoring and Security

All the company phone accounts are monitored and users shall be responsible for the use and explanation of charges when requested. Employees will be asked to justify any charges that are excessive.

Access to the internet via the phone facility is monitored, or in some cases disabled. The rules in relation to sending and receiving of emails and internet usage is detailed in the IT, Email & Internet Usage Policy.

