POLICY FOR THE APPROPRIATE AND FAIR USE OF COMPANY MOBILE PHONE AND SIMILAR COMMUNICATION DEVICES

Introduction:

AFE Group recognises that to ensure the most effective running of its business activities and communications it is necessary for some staff to have access to mobile communication devices. This policy and related procedures set out a protocol for the permitted work related use of mobile technology, and indicate ways in which mobile technology could assist in more flexible working within our business. The policy should be applied consistently to all AFE Group employees so as to ensure the correct and proper use of AFE Group assets and funds.

Related Policies:

The policy should also be read in conjunction with the work related road safety policy, AFE Group driver handbook, travel expenses policy and company car phone policy. These policies set out procedures for safe and legal use and highlight the need for minimising distractions, accident risk, and frustrations that inappropriate and improper use can cause. Matters of data protection and privacy are covered under the company's GDPR policies.

Conditions of Use

The Company recognises that mobile devices are essential work tools and provide a very effective means of communication between colleagues, customers and other business stakeholders. It is further acknowledged that such devices are an important tool to support lone workers, those working on call or when working in remote locations. Mobile device users should not download third party software, ringtones or any mobile apps without the prior permission of the IT department. All users must adopt practices of fair and reasonable use, with devices only for use by the employee to whom it was issued. Employees should safely use mobile devices, and only use secure connections so as to protect the device and company IT systems from cyber risks.

Fair and Appropriate Usage (including incidental personal use)

The Company recognises that on occasions, mobile device users may need to make use of the Company device for personal reasons. Occasional personal use should be kept to a fair and appropriate level. Any excessive use of voice calls and data may result in The Company recovering these costs from the user.

The following are principal examples of appropriate business related use:-

- 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
- For photographing or video taking of work related activities (eg appliance or component part ID, site survey reporting, competitor product evaluation etc)
- To schedule and keep track of appointments
- To carry out work-related research

- To keep track of work tasks and work contacts
- For authorised work related social media broadcasting that solely and professionally promotes the company brand reputation, product and business interest.
    - Company mobile phones and similar devices should not be used for personal surfing of the internet, personal banking, personal social media; video, music streaming, or gaming.
    - Incidental private use will be fairly interpreted and applied by the company recognising the individual user's working hours, travel obligations and place of work. An appropriate fair and reasonable dispensation will be made for employees working overseas on business.

An employee may still be subject to a HMRC Benefit in Kind tax charge unless it can be demonstrated that the mobile device is provided to an employee solely for business use and that any private use is not significant.

The company receives detailed reporting of air time, data use and costs from the service provider. Such reports will be made available to the user to support any actions taken under this policy.

User Responsibilities

It is the responsibility of the user to ensure the security, proper usage and maintenance of any device issued. The mobile device must only be used for business purposes with the exception of use in emergencies and incidental personal use.

The following are examples of responsibilities that users should uphold at all times:-

For your safety and that of others –

- Mobile devices should not be used when they could pose a security or safety risk, or when they distract from work tasks
- The use of mobile phones (unless safe to do so and in an appropriate hands free kit) are expressly prohibited whilst driving
- Never use a mobile device while operating equipment.

For reasons of data privacy and cyber security:–

- Do not use work mobile devices for personal tasks
- Do not use personal mobile devices for work tasks
- Do not use mobile devices to record confidential information
- Never remove the SIM and place into another device, unless instructed to by the IT Department
- Ensure that your device has a security pass code so as to prevent unauthorised access and use.

.

For good business standards and conduct during meetings you should –

- Avoid where possible to use mobile devices during meetings
- Comply with any restrictions of use that may be set – for example in Trains, Airports or other such locations.
- Avoid using your device in anti social hours or outside of necessary or appropriate working hours

Managing mobile device security and vulnerability threats

AFE Group takes every care to ensure the security of all its devices and data. Cybercriminals can easily exploit vulnerabilities in mobile phones to obtain private data. These vulnerabilities sometimes come from the Apps you use or within the smart phone itself. Mobile phones are also vulnerable to malware, which can log key strokes and capture screenshots.
Users should always be vigilant in protecting their mobile devices. Apps should not be downloaded without the express permission of their IT Department. Company Mobile devices have certain pre installed Apps to assist users in efficient and cost effective communication (what's app we chat), travel and route guidance, vehicle checks, training etc.

Device users should always be careful with what emails you open, and which pictures you decide to upload. Your IT department will install a mobile device management solution to provide device security and control to help protect your device. Users should always follow IT department guidance in enabling and keeping updated both the Anti-virus software and mobile device operating system software.

Be aware of the risks in using Public Wi Fi connections and Bluetooth

It is always tempting to connect to public Wi-Fi when it is available, however, public Wi-Fi networks can make it trivial for an attacker to intercept the traffic you are sending over the unencrypted network. For this reason it is recommended to never send sensitive information over public Wi-Fi - for example, do not enter passwords or carry out internet business transactions when connected to public Wi-Fi.

Use of personal mobile telephones (BYOD – bring your own devices)

Where a member of staff does not have a company issued device or when such an issued device is not operational, the costs of business calls can be reclaimed from the company. Only cost of calls can be claimed, device rental is not a claimable cost. The cost of calls should be supported by an appropriate itemised invoice from the mobile supplier using the standard Company expenses procedure.

Personal mobile devices should be used for telephone calls only, and not connected to company IT systems without the prior permission of the IT manager. In such circumstances the company will apply device management to the personal mobile device in order to appropriately protect the company's IT systems. If continued significant business usage of a personal telephone is recorded the business unit should consider a business case for the issue of a company approved device.

International / Overseas Usage (Airtime and data roaming)

Mobile devices should not be taken outside of the UK nor used for international calling or data transmission without prior consent of The Company IT Manager and Financial Director so that these destinations can be checked for charging with the mobile carrier, and appropriate tariffs applied to the device and connection.

Damaged, Lost or Stolen Device

The user is responsible at all times for the safeguarding and security of the mobile device and it should never be left unattended.

If the device is lost or stolen, this must be reported to your manager and the IT Department immediately to ensure that the account is stopped and there is no unauthorised usage.

In the event of theft of a mobile phone, the incident must also be reported to the police and an incident number obtained (please provide this number when reporting the loss to the IT Department).

Return of mobile devices

All company mobile devices, SIMS, software and data therein remain the property of AFE Group Ltd. Should an employee be required to return any mobile device for any reason, then they should not erase any business related content.

Disciplinary Action:

Improper use of mobile phones or other mobile devices may result in disciplinary action. Continued use of mobile devices at inappropriate or anti social times or in ways that distract from work may lead to having mobile device privileges revoked.

Mobile device usage for illegal or dangerous activity, for purposes of harassment, or in ways that violate the company's policies may result in an employee facing disciplinary action.

Any fines incurred for improper use , for example, fines by train operating companies for the use of mobile devices in certain restricted areas will be payable; by the device user

Further Advice and Support

Should you require further advice and support regarding the safe and proper use of your company issued mobile phone, or clarification of this policy, please contact a member of the IT Department.