Mobile Device Usage Policy & Guidelines

1. Purpose

Mobile telephones and tablets are an integral feature of Pabulum's business operations. The purpose of this policy and procedure is to ensure that employees and workers are aware of their responsibilities when using such equipment provided by Pabulum.

2. Scope

This policy applies to:

2.1. All permanent and temporary contracted employees of Pabulum.

2.2. All forms of mobile devices provided by Pabulum including, but not limited to iPhones, Android mobiles, iPad's, Android Tablets and 3/4G Mobile Broadband devices.

3. Policy

3.1. Policy Statement

The practices and procedures set out in this document reflect the provisions set out in:

- Computer Misuse Act 1990.
- Data Protection Act 1998.
- Malicious Communications Act 1998.
- Road Vehicles (Constructions and Use) (Amendments) Regulations 2003.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

3.2. Policy Objectives

The objectives of this policy in regard to appropriate use of mobile devices and the protection of information system resources as held on or accessible from mobiles devices are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to electronic information owned by Pabulum or temporarily entrusted to it.
- Provide guidelines for professional use of mobiles devices, to ensure that they are used in such a manner that does not compromise Pabulum's business, reputation or its employees in any way.
- To outline the legal consideration that must be followed and also user responsibilities when it comes to security and appropriateness of call and call length.
- To detail the acceptable use of privately owned mobile phones for Pabulum business calls.

3.3. Policy Overview

Employees and workers must be aware of their responsibilities when using mobile devices provided by Pabulum for them to carry out their contractual requirements. This policy clarifies the boundaries of personal use and underlines the seriousness which Pabulum view inappropriate, unlawful or malicious use of the mobile devices provided.

Users are expected to observe the arrangements set out in this policy and procedure and to report to line management any circumstances where they believe mobile devices are not being used appropriately.

3.4. Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an on-going basis by Pabulum. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of email or other relevant communication.

Users shall then have the obligation to obtain the current information systems policies from Pabulum's network storage facilities on an on-going basis and accept the terms and conditions contained therein.

4. Policy Requirements

4.1. User Responsibilities

Where a mobile device allows access to the internet any use of that facility is governed by the following Pabulum policies:

- IT Policy
- GDPR Policy

The user should take reasonable steps to prevent damage or loss to their mobile device. This includes not leaving it in view in an unattended vehicle(s) and storing it securely when not in use. The user may be responsible for any loss or damage if reasonable precautions are not taken.

In general, mobile devices will only be provided for work related purposes. However, it is recognised that there may be a need to make and receive occasional private calls.

Cost and usage are monitored and where excessive personal use is identified costs will have to be reimbursed. Pabulum will determine what constitutes excessive personal use.

The mobile device is always, the property of Pabulum and must be surrendered on request for any reason.

4.2. Pabulum Responsibilities

Pabulum is responsible for:

- Purchasing and allocation of mobile devices.
- Maintaining a library of all Pabulum mobile device assets.
- Disposal of all mobile devices.

4.3. Privacy and Dignity

Mobile devices having the capability of taking still images or video footage represent a potential threat to the privacy and dignity of both employee, advisers and members of the public. No still image or video footage may be taken without their express consent. Images of unit service areas may be taken on site visits, general inspection or health & safety inspections with mobile device, but these must not include identifiable images of individuals without their express consent first being obtained. In no instance whatsoever may still images or video footage taken with Pabulum mobile devices be posted onto the internet or social media sites without the appropriate authority being first obtained.

4.4. Security Requirements

Pabulum employees must take care of any mobile devices assigned to them. All such devices must be password protected and not used in public places without due care and attention by the employee. All mobile devices, namely referring to mobile phones, iPad's and Android Tablets are assigned a default password at the time of the mobile device being assigned to an employee. The obligation is with the employee to ensure that the password is changed within a reasonable timeframe upon receiving the mobile device and meets the guidelines set out by Pabulum. Devices must be set with a minimum of 6 characters and must be changed every 3 months.

All lost, stolen or mislaid mobile devices are to be reported immediately to the Finance Director and IT@pabulum-catering.co.uk as soon as practical and obtain a policy case reference number.

All security incidents, including actual or potential unauthorised access to Pabulum's information systems, must be reported immediately to the Finance Director and IT@pabulum-catering.co.uk.

Mobile devices that are lost or otherwise compromised through persistent lapses in security by the employee may incur costs to the user in respect of replacement charges or, in extreme cases, availability may be withdrawn.

4.5. Safety

Caution should be exercised in the use of mobile phones, avoiding long duration phone calls, texting or emailing where possible.

4.6. Driving

Pabulum discourages the use of mobile devices whilst driving.

Where a driver must take a call, they should ensure that they comply with the law and that any hands-free device used is compliant with current legislation. Calls should be kept short and where possible arrangements should be made to continue it when the driver is parked safely and legally.

At all times drivers should keep their concentration on the road and ensure that they drive with due care and attention to themselves and other road users.

Whenever possible, drivers should let incoming calls go to their voicemail and then a find a safe, legal, place to park, switch off their engine and respond to the call.

On no account should any Pabulum employee use mobile devices other than hands-free whilst driving.

4.7. Acceptable Use

All employees are expected to use mobile devices provided by Pabulum in an appropriate, acceptable and reasonable manner in accordance with the terms outlined herein this document and appendixes expected to exercise good sense and responsibility in limiting any personal use of their mobile devices to a minimum and refrain from any inappropriate use. The following list gives examples of inappropriate use of Pabulum mobile devices:

- Communications to premium rate numbers e.g. 0870, 0845.
- Communications to social media sites not related to Pabulum.
- Communications to votes of TV / Radio programmes.
- Communications involving bidding in online auctions.
- Communications involving betting / competitions.
- Communication that are illegal, obscene or libellous.
- Communication that are offensive or threatening.
- Communications that infringe copyright laws.
- Communications that transmit spam, chain or junk messages.
- Accessing websites that are not essential for the better conduct of Pabulum's business.
- Any other use that might cause commercial, reputational or financial distress to Pabulum.

Employees are reminded that emails and text messages sent on Pabulum mobile devices are admissible in court and subject to Data Protection and Freedom of Information legislation and therefore they could possibly be released into the public domain or to individuals mentioned in them.

Employees found using their mobile devices in an inappropriate manner may have their mobile devices withdrawn and be subject to disciplinary action.

4.8. Use of Privately Owned Mobile Devices

Connection of personal equipment to Pabulum's information systems will be at the sole risk of the person wishing to do so and subject to conforming to all policies as if the device were owned by Pabulum.

Support and assistance for personal equipment will only be provided on a 'best endeavours' basis.

Personal equipment which has been connected to Pabulum's information systems and then lost will be considered a security incident and reported to the Finance Director and IT@pabulum-catering.co.uk as soon as possible.

It is the responsibility of the owner of the equipment to contact their service provider as soon as possible and request the equipment be terminated remotely.

4.9. Usage Charges

Line Managers will have responsibility for keeping control of mobile device usage by identifying those individuals who use a mobile device excessively and taking steps to reduce this.

Bills for mobile devices will be issued monthly to the finance department for processing.

Usage charges are currently paid by Pabulum, but the finance team are responsible for flagging any inconsistencies or fluctuations within the mobile device invoice with the Finance Director.

The allocation of talk time is currently unrestricted due to the contract type offering unlimited calls to standard UK mobile numbers beginning with 07 and UK landlines.

The allocation of mobile data is capped per user up to 5gb per mobile phone with a reset date of the 1st of each month. Any mobile phone which uses its data allocation will be reviewed and increased, if necessary, on a temporary basis by the Finance Director. This does not affect the mobile phone from being used to access wireless connections to gain an internet connection.

The use of text messaging is strictly for business communication and should not be used to engage in personal communication which can be deemed as inappropriate, intrusive or abusive to the individual receiving the text communication.

4.10. Personal Data

Employees have the general right, under the Data Protection Act, to receive, on written request, a copy of any personal data concerning them, including information held electronically on systems owned by Pabulum, including mobile devices. There are a few limited exceptions to this such as data held for crime prevention / detection purposes, but most individuals will be able to have a copy of the personal data held on them.

5. Disciplinary Process

It remains the ultimate responsibility of the individual and their managers to ensure that the business and privately owned mobile devices are used appropriately. Any misuse may constitute a breach of policy and as such the individual committing the misuse may be subject to disciplinary procedures.

6. Deviations from Policy

Unless specifically approved by the Finance Director, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the Finance Director.

Nelson Williams
Managing Director
(This policy will be reviewed in February 2024)

APPENDIX A – List of Related Documents, Procedures and Processes

To cover in IT Policy

- Access Control Policy & Guidance
- Internet Usage Policy & Guidance
- Wireless Communications Policy & Guidance
- Lost or Stolen Hardware Process
- Electronic Communications Acceptable User Policy & Guidance
- Security Breach & Weakness Policy & Guidance

Policies to consider

- Pabulum's Rules and Disciplinary Code
- End User Acceptable Use Policy & Guidance

Legislations / Regulations / Acts

- Computer Misuse Act 1990
- Malicious Communications Act 1998
- Road Vehicles (Construction and Use) (amendments) Regulations 2003
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Data Protection Act
- Data Protection Act - Statement