Mobile Device Policy

Version 25th Feb 2024

For the purposes of this policy, where the term Elysian is used, it refers to Elysian Animal Assisted Interventions Ltd including Elysian School and Elysian Animal assisted Therapy and Learning.
This policy is applicable to all Elysian sites.

The purpose of this policy and procedure is to ensure that employees are aware of their responsibilities when using mobile device equipment provided by Elysian Animal Assisted Interventions Ltd. Mobile telephones and tablets/ipads are referred to, as "mobile devices" in this document.

Scope

This policy applies to:

1. All permanent and temporary employees and any other third parties using equipment provided by Elysian.
2. All forms of mobile devices within the organisation including, but not limited to all mobile phones including non-internet connected devices, all tablets including Wi-Fi and sim connected devices.

Policy Statement

The practices and procedures set out in this document reflect the provisions set out in the Computer Misuse Act 1990, the Data Protection Act 1998, the General Data Protection Regulation (as of May 2018), the Malicious Communications Act 1998, the Road Vehicles (Construction and Use) (amendments) Regulations 2003 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Objectives

The objectives of this policy:

1. Define and set out the appropriate use of mobile devices.
2. Ensure the protection of information held on or accessible from mobile devices.
3. Ensure the Company and its staff minimises the threat of accidental, unauthorised, or inappropriate access to electronic information owned by the organisation or information temporarily entrusted to it.
4. Provide guidelines for professional use of mobile devices, to ensure the devices are used in such in a way that does not compromise the organisation or its employees in any way.
5. Detail the mobile devices available to order, the process for obtaining a device and monthly costs associated with a mobile device.
6. Set out possible outcomes if the mobile device is used incorrectly and what process to follow if a device is lost or stolen.

Requirements

1. Users must be aware of their responsibilities when using mobile devices provided by Elysian.
2. Users must be aware of the bounds of personal use and the seriousness with which the organisation views the inappropriate, excessive, unlawful, or malicious use of the mobile devices provided.
3. Users are expected to observe the arrangements set out in this policy and to report any circumstances where they believe mobile devices are not being used appropriately to line management or the leadership team.
4. Where a mobile device allows access to the internet, any use of that facility is governed by Elysian's policies.
5. The user should take reasonable steps to prevent damage or loss to their mobile device. This includes not leaving it in view in unattended vehicles and storing it securely when not in use. The user may be responsible to the Organisation for any loss or damage if reasonable precautions are not taken. Staff are responsible for protecting any mobile devices with appropriate covers, including screen cvoers.
6. Users must not re-allocate mobile devices to others without first seeking authorisation from the organisation. In the event this change is authorised, all elements of the contract including phone number will also be transferred and should be acknowledged and signed for by the users. The transfer will be managed by the administrative support or leadership team to ensure the system is updated with the new owner's information.
7. The mobile device is, at all times, the property of Elysian and must be surrendered on request for any reason. The organisation has the right to access content on mobile devices.
8. Mobile devices have the capability of taking still or moving images. This represents a potential threat to the privacy and dignity of those both internal and external to the Organisation. No still or moving images of individuals may be taken without their express consent. No still or moving images taken with the organisation mobile devices are to be posted onto the internet / social media sites without appropriate authority being first obtained.
9. The organisation discourages the use of mobile devices whilst driving. Where a driver must take a call, they should ensure that they comply with the current legal position and ensure that any hands free device used is legally compliant. On no account should any Elysian employee use mobile devices other than hands free whilst driving. Conference calls should not be conducted whilst driving.

Acceptable use

All employees are expected to use mobile devices provided by the Organisation in an appropriate, acceptable and reasonable manner in accordance with Elysian Policy and procedures. Employees are 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 (non-exhaustive) examples of inappropriate use of organisation mobile devices:

1. Communications to premium rate numbers
2. Communications to votes of TV/radio programmes.
3. Communications involving bidding in online auctions.
4. Communications to betting sites/competitions.
5. Communications that are illegal, obscene, libellous or slanderous
6. Communication that are offensive or threatening

7. Communications that infringe copyright
8. Communications that transmit unsolicited commercial or advertising material
9. Communications that transmit spam, chain, or junk messages
10. Any other use that might cause commercial, reputational or financial distress to the organisation.
11. 11. Excessive use (including excessive use both within and outside of the user's working hours)
12. Any communication or action, which would contravene Elysian's policies and procedures.

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

Users found using their mobile devices in an inappropriate manner might have their mobile devices withdrawn and be subject to disciplinary action under the Organisation's Disciplinary Procedure (or other relevant procedure).

Cost and usage are monitored and where excessive personal use is identified, costs may have to be reimbursed to the Organisation. The Organisation will determine what constitutes excessive personal use depending on Particular circumstances.

Mobile Devices

Elysian will offer a good model of current iPhone/iPad ranges (e.g. iPhone 7). Requests for alternative devices is not possible.

Costs

The contracted mobile phones are on a 10GB data, unlimited calls, and texted, capped spending contract, paid for by the organisation. A replacement handset may be provided If there is a fault with the phone. Replacement handset will not be provided in case of accidental breakage where the phone has not been adequately protected, and the employee may occur a cost for a replacement handset. The organisation will provide a new sim card.

Roaming in the EU is now charged at UK data rates however, you will need to check your destination in Europe is in the EU, as charges will apply for countries outside of the EU in Europe. Please note calls made from ships and cross channels ferries will not be covered under the EU roaming policy and will be charged.

Insurance

The mobile phones are not insured, and staff are responsible for the maintenance and protection of their allocated phone.

Data

Users have the 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 the University 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.

Safety

Caution should be exercised in the use of mobile devices avoiding long duration phone calls, texting or emailing where possible with regular breaks from screens as needed.

Security

All mobile devices must be password protected and not used in public places without due care and attention by the user.

All lost, stolen, or mislaid mobile devices are to be reported immediately to the administrative support and leadership team as soon as practicable. The user must also report the loss to police as soon as practicable and obtain a case reference number.

All security incidents, including actual or potential unauthorised access to the organisation's systems, must be reported immediately to the administration and leadership team.

Mobile devices that are lost or otherwise compromised through lapses in security by the employee may incur costs in respect of replacement or device or call charges, which will be recharged to the user. The mobile device may be removed at any time if this policy is breached.

Confirming receipt of phone and acceptance of policy

Employee Sign:

Employee print name:

Date: