**Posture And Mobility Group Security Statement**

**1. Introduction**

**Why have we produced this document?**

This document details the organisational and technological measures that we have put into place to ensure that we comply with the General Data Protection Regulation and any subsequent UK data protection laws (“the data protection legislation”) and also as necessary to protect our business, systems, information and employees.

In addition, we must ensure that we monitor those measures so that they are properly implemented and remain effective to meet their intended objectives.

**What other policies apply?**

We have other important policies and other documentation that you should read, these are our:

* Privacy Policy;
* Personal Data Breach Policy and Procedure; and
* Individual Requests Procedure (Subject Access Requests etc).

**Who is responsible for Security?**

**Senior Members of Staff**

Both day-to-day responsibility as well as ultimate responsibility for security rests with Olwen Ellis (“the PMG Manager”) who shall manage, implement and update policies and related procedures.

Line managers are responsible for ensuring that both permanent and temporary staff and contractors are aware of:

* The security policies applicable to the services and systems they use;
* Their personal responsibilities for security; and
* How to access advice on security matters.

**All Staff**

All staff shall comply with security policies and procedures. Failure to do so can have consequences, such as disciplinary action. Contracts of employment also contain confidentiality and data protection provisions that all staff must adhere to.

Each member of staff is responsible for the operational security of the services and systems they use, and all staff members must undertake data protection training and any specific training as directed by the organisation.

**Contractors and agency staff**

If the organisation needs to use contractors or agency staff, the contracts with the contractor or agency staff will ensure that they comply with appropriate confidentiality provisions, this policy and the data protection legislation.

**2. Security measures and your technology**

**Managing the organisations assets**

**Asset Ownership**

It is important to ensure that information assets (e.g. hardware, software, applications or data) have staff members designated to be responsible for the information security of each asset.

**Asset Records and Management**

the PMG Manager shall keep an accurate record of business information assets, including acquisition, ownership, modification and disposal. Material such as licenced software, confidential information and personal data should be removed from hardware before disposal and its removal should be reported to the PMG Manager.

**Removable media**

Removable media should be monitored and its use only permitted with the permission of the appropriate line manager and the PMG Manager who will ensure it is safe and secure to use. The use of removable media will be restricted to where absolutely necessary and must be encrypted if personal data is to be stored on it.

**Mobile devices (e.g. phones, tablets, laptops etc.)**

Use of mobile devices for business purposes is only permitted where the device is issued by the organisation or with the permission of the appropriate line manager and the PMG Manager, if privately owned. The organisation will ensure that business mobile devices are adequately protected and staff should not attempt to circumvent any security measures put into place on devices issued to them.

Where a device is privately owned it must have installed appropriate virus protection that is updated regularly. It must have pin, password or other authentication installed, be encrypted wherever possible and be capable of being remotely tracked and wiped.

Staff must inform the PMG Manager as soon as they become aware if the device is lost or stolen (whether business or privately owned) and the device must be completely wiped remotely.

**3. Access Management**

**Physical Access**

Only authorised staff should be given access to business premises containing information systems or stored data. Staff members will be issued with a security pass (if appropriate) and shall not permit access to any person who does not have a security pass or who cannot show a valid business reason to be at the premises.

**User Access to Systems and Services**

Access to systems should be restricted to authorised staff who have a bona-fide business need to use the system. The staff members will be issued with a password which will limit their system access to that necessary in order for that staff member to perform their role.

**Hardware Access**

**System Perimeter access**

The boundary between the systems and the internet shall be protected by a firewall, which shall be configured to meet the threat and continuously monitored and virus protection shall be in place.

the PMG Manager shall be responsible for maintaining the system perimeter access.

**Monitoring System Access and Use**

An audit trail of system access by staff should be maintained wherever practical and reviewed on a regular basis by the PMG Manager.

**Physical and Environmental Management**

In order to minimise loss of, or damage systems, the organisation shall put into place measures to ensure that equipment is physically protected from threats.

The organisation will put into place appropriate measures to protect systems from power loss.

**4.) Computer and Network Procedures**

**Updates**

The organisation shall ensure that hardware and software is updated in accordance with the recommendations of suppliers and any changes made to systems, applications or networks should be subject to approval by the PMG Manager.

The systems will be set to receive automatic updates.

**Local Data Storage**

[Amend as appropriate suggestion below]

Data stored on the business premises should be backed up regularly in accordance with the table below:

[insert backup details]

Name of System Who is responsible How often backed up

The backup copy should be held in a different physical location as agreed with [insert job title] and the Data Protection Officer.

**External Providers**

The organisation uses data storage, applications or other services are provided by other organisations. These organisations have provided evidence that they have the necessary technological and organisational procedures in place to protect systems and personal data and we have entered into contractual arrangements with them to this effect.

**Passwords**

All passwords should be changed from the original and only strong passwords should be used. They will be at least 8 characters.

Passwords should not be written down or must not be shared. Staff members may use LastPass® to store passwords so that they only need to remember one master password.

Whenever a staff member leaves the organisation, their access to systems and services should be terminated within 4 days of their leaving

**Data Security Breaches**

All breaches of this security policy should be reported to the PMG Manager who will decide whether to investigate the breach in line with the Data Breach Policy where necessary.

**Business Continuity and Disaster Recovery Plans**

The organisation has in place business impact assessment, business continuity and disaster recovery plans for all mission critical information, applications, systems and networks.

**5.) Email Security**

The organisation does not routinely use email as a method of sending personal data, however, if it is necessary to do so then that email should be encrypted or password protected. the PMG Manager should be consulted if a member of staff is aware of a situation where email is being used routinely to send personal data.

The ‘*bcc’* function will be used by staff to hide email address when emailing multiple recipients and the auto complete function may be only be used where a staff member has double checked that the email is going to the correct recipient.

The organisations spam software should remove most spam, but staff members have been advised not to not open spam emails or any suspicious looking emails. If in doubt they must consult the PMG Manager.

The procedures above must be followed in respect of passwords.