Acceptable IT Usage Policy

This Acceptable IT Usage Policy covers the security and use of all PBE's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all PBE employees, contractors and volunteers.

This policy applies to all information, in whatever form, relating to PBE's business activities, and to all information handled by PBE relating to other organisations with whom it deals. It also covers all IT facilities operated by PBE or on its behalf.

PBE will provide access to an IT support company who will provide an IT helpdesk and should be contacted with any issues encountered while using PBE IT systems. Speak to the Operations and Finance Manager for contact details.

Computer Access Control – Individual's Responsibility

Access to the PBE IT systems, including any cloud based systems, are controlled by the use of user IDs and passwords. All user IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all their actions on PBE's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any PBE IT system
- Leave their user accounts logged in at an unattended and unlocked computer
- Use someone else's user ID and password to access PBE's IT systems
- Leave their password unprotected (for example by writing it down)
- Perform any unauthorised changes to PBE's IT systems or information
- Attempt to access data that they are not authorised to use or access
- Connect any non-PBE authorised device to the PBE network or IT systems
- Store PBE data on any unauthorised equipment
- Give or transfer PBE data or software to any person or organisation outside PBE without the authority of PBE

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to the IT systems and data.

Internet and Email Conditions of Use

Use of PBE internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to PBE in any way, is not in breach of any terms and condition of employment and does not place the individual or PBE in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse
- Use profanity, obscenities, or derogatory remarks in any communications
- Access, download, send or receive any data (including images) which PBE considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material
- Use the internet or email to make personal gains or conduct a personal business
- Use the internet or email to gamble
- Use the internet or email systems in a way that could affect its reliability or effectiveness
- Place any information on the internet that relates to PBE, alter any information about it, or express any opinion

about PBE, unless they are specifically authorised to do so

- Send unprotected sensitive or confidential information externally
- Forward PBE email to personal (non-PBE) email accounts
- Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
- In any way infringe any copyright, database rights, trademarks or other intellectual property
- Download any software from the internet without prior approval of the Operations and Finance Manager.
- Particular care must be taken when connecting PBE devices to the internet using non-standard connections such as Wi-Fi hotspots or Bluetooth.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, PBE enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended
- Care must be taken to not leave confidential material on printers or photocopiers
- All confidential business-related printed matter must be disposed of using confidential waste bins or shredders

Remote Working

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- When accessing PBE systems from a home or work laptop, you must ensure that adequate protection is in place and no unauthorized users have access to PBE systems
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car
- Laptops must be carried as hand luggage when travelling
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must only be used in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only PBE authorised mobile storage devices should be used when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by PBE on PBE's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on PBE computers must be approved and installed by PBE.

<u>Individuals must not:</u>

Store any personal files on PBE equipment.

Viruses

PBE have implemented centralised, automated virus detection and virus software updates. All laptops have antivirus

software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software
- Attempt to remove virus-infected files or clean up an infection, other than by approved PBE anti-virus software and procedures

Telephone Equipment

Use of PBE telephone equipment is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to PBE in any way, is not in breach of any terms and conditions of employment and does not place the individual or PBE in breach of statutory or other legal obligations. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Make hoax or threatening calls to internal or external destinations
- Accept reverse charge calls from domestic or international operators, unless for business use

Actions upon Termination of Contract

All PBE equipment and data, including laptops, mobile devices, telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to PBE at termination of contract.

All PBE data or intellectual property developed or gained during the period of employment remains the property of PBE and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on PBE computers is the property of PBE and there is no provision for individual data privacy, however wherever possible PBE will avoid opening personal emails.

IT system logging will take place and where reasonable suspicion exists of a breach of this or any other policy PBE will investigate. PBE has the right to monitor activity on its systems, including internet, email and telephone use, in order to ensure security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

It is your responsibility to report suspected breaches of this policy to your line manager and / or the Operations and Finance Manager.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with PBE disciplinary procedures.