# Data protection policy for PMEC

## Context and overview Key details •Policy

prepared by: Hannah Herbert on: 27/05/2023 •Next review date: 27/05/2034

## Introduction

PMEC needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored— and to comply with the law.

## Why this policy exists

This data protection policy ensures PMEC Complies with data protection law and follow good practice •Protects the rights of staff, customers and partners and protects itself from the risks of a data breach

## Data protection law The General Data Protection

Regulation2018 describes how organisations PMEC— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The General Data Protection Regulation is underpinned by eight important principles. These say that personal data must: 1.Be processed fairly and 2

lawfully .Be obtained only for specific, lawful purposes 3.Be adequate, relevant and not excessive
3 4.Be accurate and kept up to date 5.Not be held for any longer than necessary 6.Processed in accordance with the rights of data subjects 7.Be protected in appropriate ways 8.Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

## People, risks and responsibilities Policy scope

This policy applies to: PMEC •All branches of PMEC•All staff and volunteers of PMEC•All contractors, suppliers and other people working on behalf of Impulse PMEC. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018. This can include: •Names of individuals •Postal addresses •Email addresses •Telephone numbers

## Data protection risks

This policy helps to protect PMEC from some very real data security risks, including: •Breaches of confidentiality. For instance, information being given out inappropriately. •Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them. •Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with PMEC has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility: •The company owner Hannah Herbert is responsible for ensuring that PMEC meets its legal obligations. All data protection procedures and related

policies, in line with an agreed schedule. Arranging data protection training and advice for the people covered by this policy. Handling data protection questions from staff and anyone else covered by this policy.Dealing with requests from individuals to see the data PMEC holds. Checking and approving any contracts or agreements with third parties. Hannah Herbert is also responsible for: Ensuring all systems, services and equipment used for storing data meet acceptable security standards. Performing regular checks and scans to ensure security hardware and software is functioning properly. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services, any data protection statements attached to communications such as emails and letters. Addressing any data protection queries from journalists or media outlets like newspapers. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## General staff guidelines

•The only people able to access data covered by this policy should be those who need it for their work. •Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers. PMEC will provide training to all employees to help them understand their responsibilities when handling data. •Employees should keep all data secure, by taking sensible precautions and following the guidelines below. •In particular, strong passwords must be used and they should never be shared. •Personal data should not be disclosed to unauthorised people, either within the company or externally. •Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. •Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason: When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.