****

**Data Protection and Confidentiality Policy**

**October 2024**

**1. Purpose**

Pembroke Street EMB (PEMB) is a Tenant Management Organisation which is committed to ensuring the protection and confidentiality of personal data in compliance with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). This policy outlines the procedures for collecting, storing, processing, and sharing personal data, ensuring that the rights of individuals are upheld and that personal information is handled with care and confidentiality.

**2. Scope**

This policy applies to all employees, volunteers, contractors, board members, and any other parties handling personal data on behalf of the Tenant Management Organisation (TMO). It covers the processing of personal data related to tenants, employees, volunteers, contractors, suppliers, and any other individuals whose personal data is held by the TMO.

**3. Data Protection Principles**

In accordance with the GDPR, the TMO commits to handling personal data in accordance with the following key principles:

1. **Lawfulness, Fairness, and Transparency**
Personal data will be processed lawfully, fairly, and in a transparent manner. Individuals will be informed of how their data is used, with clear and understandable privacy notices.
2. **Purpose Limitation**
Personal data will only be collected for specified, explicit, and legitimate purposes and will not be processed for purposes that are incompatible with those purposes.
3. **Data Minimisation**
The TMO will only collect and process personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. **Accuracy**
The TMO will take reasonable steps to ensure that personal data is accurate and kept up to date. Inaccurate data will be corrected or erased promptly.
5. **Storage Limitation**
Personal data will be kept for no longer than necessary for the purposes for which it is processed.
6. **Integrity and Confidentiality**
The TMO will put in place measures to ensure that personal data is processed securely, protecting it from unauthorised access, disclosure, or destruction through appropriate technical and organisational measures.
7. **Accountability**
The TMO will be accountable for complying with these principles and will be able to demonstrate compliance with its data protection obligations.

**4. Data Collection and Processing**

**4.1 Lawful Basis for Processing**
The TMO will only process personal data where a lawful basis for processing exists. These include:

* **Consent:** The individual has given clear consent for the processing of their personal data.
* **Contractual Obligation:** Processing is necessary for the performance of a contract to which the data subject is a party.
* **Legal Obligation:** Processing is necessary for compliance with a legal obligation.
* **Legitimate Interests:** Processing is necessary for the purposes of legitimate interests pursued by the TMO, provided these do not override the rights and interests of the data subject.

**4.2 Special Category Data**
Special category data, such as health information or ethnicity, will be processed only where it is necessary and where a specific lawful condition applies, such as explicit consent, employment law, or vital interests.

**5. Data Subject Rights**

The TMO respects the rights of individuals regarding their personal data. These rights include:

1. **Right to be Informed**
Individuals have the right to be informed about the collection and use of their personal data. The TMO will provide clear and concise information through privacy notices.
2. **Right of Access**
Individuals have the right to access their personal data held by the TMO and receive information about how it is processed. Requests will be responded to within one month of receipt.
3. **Right to Rectification**
Individuals have the right to request the correction of inaccurate personal data or the completion of incomplete data.
4. **Right to Erasure (Right to be Forgotten)**
Individuals can request that their personal data be deleted, provided there is no lawful reason for the TMO to retain it.
5. **Right to Restrict Processing**
Individuals have the right to request the restriction or suppression of their personal data in certain circumstances.
6. **Right to Data Portability**
Individuals can request to receive their personal data in a commonly used format, allowing them to reuse it across different services.
7. **Right to Object**
Individuals can object to the processing of their personal data in certain situations, including direct marketing.
8. **Rights in Relation to Automated Decision Making and Profiling**
The TMO does not engage in automated decision-making or profiling without human intervention.

**6. Data Security**

**6.1 Physical Security**

* Personal data stored in physical form (e.g., paper files) will be kept in secure, locked locations with restricted access.
* Access to these areas will be limited to authorised personnel only.

**6.2 Digital Security**

* Personal data stored electronically will be protected through the use of secure passwords, encryption, firewalls, and other appropriate security measures.
* Access to data will be restricted based on role and necessity.
* Regular data backups will be taken to ensure the security of stored information in case of system failures.

**6.3 Data Breach Response**

* Any data breaches, including the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to personal data, must be reported immediately to the TMO Manager and the Board od Directors.
* In the event of a breach, the Manager will assess the risk to individuals and, where necessary, report the breach to the Information Commissioner’s Office (ICO) within 72 hours.
* Affected individuals will be notified where there is a high risk to their rights and freedoms.

**7. Sharing Personal Data**

* **Third-Party Data Sharing:**
Personal data will only be shared with third parties where necessary for the purposes of fulfilling the TMO’s functions (e.g., contractors, local authorities) and where a lawful basis for sharing exists.
* **Data Sharing Agreements:**
Where data is regularly shared with third parties, a data-sharing agreement or contract will be put in place to ensure that the data is processed in compliance with GDPR and this policy.
* **International Transfers:**
Personal data will not be transferred outside the UK or European Economic Area (EEA) unless appropriate safeguards are in place.

**8. Confidentiality**

* **Employee and Volunteer Obligations:**
All employees, board members, and volunteers must respect the confidentiality of personal data and sensitive information they handle in their roles. They must not disclose personal data or confidential information to unauthorised individuals, either inside or outside the organisation.
* **Confidentiality Agreements:**
Employees and volunteers will be required to comply with the confidentiality policy upon joining the TMO to ensure they understand their responsibility in protecting confidential information.
* **Disclosures:**
Personal data will not be disclosed to third parties without the explicit consent of the individual unless required by law or in the event of an emergency where disclosure is necessary to protect the vital interests of the individual.

**9. Data Retention**

* **Retention Periods:**
Personal data will only be retained for as long as necessary to fulfil the purposes for which it was collected or as required by law.
* **Secure Disposal:**
Once personal data is no longer required, it will be securely destroyed, whether stored electronically or in physical form. Electronic data will be securely deleted, and paper records will be shredded or incinerated.

**10. Training and Awareness**

* All employees and volunteers handling personal data will receive appropriate data protection training. This training will be updated regularly to reflect changes in legislation or policy.
* Employees and volunteers will be made aware of the importance of confidentiality and the procedures for safeguarding personal data.

**11. Roles and Responsibilities**

**11.1 Data Protection Officer (DPO)**
The TMO appoints the EMB Manager as Data Protection Officer (DPO) who will:

* Oversee the implementation of this policy and ensure ongoing compliance with data protection laws.
* Act as the point of contact for any data protection queries, subject access requests, or data breach reports.
* Liaise with the Information Commissioner’s Office (ICO) when necessary.

**11.2 Employees and Volunteers**

* All employees, board members, and volunteers are responsible for complying with this policy and protecting the confidentiality of personal data they handle.
* They must report any data breaches, potential breaches, or security concerns immediately to the DPO.

**12. Monitoring and Review**

This Data Protection and Confidentiality Policy will be reviewed annually or more frequently if required by changes in legislation or operational needs. The Board of Directors will approve any revisions to ensure the policy remains effective and compliant.

By following this policy, Pembroke EMB aims to ensure that personal data is processed legally, fairly, and securely, protecting the privacy and rights of individuals while maintaining the confidentiality of sensitive information.