# Pembroke EMB Ltd
# Data Protection and Confidentiality Policy (GDPR)

## 1. Purpose

**1.1** Pembroke Street EMB (PEMB) is committed to protecting personal data and handling it responsibly in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR) (where applicable)

**1.2** This policy sets out how PEMB collects, uses, stores, shares, and protects personal data, and ensures individuals' rights are upheld.

## 2. Scope

**2.1 This policy applies to:**

- Employees
- Volunteers
- Board members
- Contractors and third parties acting on behalf of PEMB

**2.2** It covers all personal data processed by PEMB, including data relating to:

- Tenants and residents
- Staff and volunteers
- Contractors and suppliers
- Service users and stakeholders

## 3. Definitions

3.1 **Personal Data**: Any information relating to an identifiable individual.
3.2 **Special Category Data**: Sensitive data (e.g. health, ethnicity, religion).
3.3 **Processing**: Any operation performed on personal data (collection, storage, use, deletion).
3.4 **Data Controller**: PEMB determines how and why personal data is processed.
3.5 **Data Processor**: A third party processing data on behalf of PEMB.

## 4. Data Protection Principles

**4.1** PEMB complies with UK GDPR principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

## 5. Lawful Basis for Processing

**5.1** PEMB will identify and document a lawful basis before processing personal data:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

**5.2 Legitimate Interests Assessments (LIAs)** will be completed where this basis is used.

## 6. Special Category Data

**6.1** Special category data will only be processed where:

- A lawful basis applies **AND** a condition under Article 9 UK GDPR is met

**6.2** Additional safeguards will be implemented, including restricted access and enhanced security.

## 7. Data Subject Rights

7.1 Individuals have the following rights:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making

**7.2** Requests will be handled within **one calendar month**.

**7.3** PEMB will maintain a **Subject Access Request (SAR) procedure and log**.

## 8. Data Collection and Transparency

**8.1** PEMB will provide **privacy notices** that clearly explain:

- What data is collected
- Why it is collected
- Legal basis
- Retention periods
- Rights of individuals

**8.2** Privacy notices will be:

- Clear and accessible
- Provided at the point of data collection

## 9. Data Security

**9.1 Technical and Organisational Measures**

PEMB will implement appropriate measures including:

- Access controls (role-based access)
- Encryption and secure systems
- Password policies and MFA where possible
- Secure backups
- Device and network security

## 9.2 Physical Security

- Locked storage for paper records
- Restricted access to offices and filing systems

**9.3 Staff Responsibilities**

All staff must:

- Keep data secure
- Not share passwords
- Report incidents immediately

## 10. Data Breach Management

**10.1** All data breaches must be reported immediately to the DPO/Manager.

**10.2** PEMB will:

- Assess risk
- Record all breaches in a **breach log**
- Report to ICO within **72 hours** if required
- Inform affected individuals where there is high risk

**10.3** A **Data Breach Procedure** will be maintained.

## 11. Data Sharing

**11.1** Personal data will only be shared where there is a lawful basis and it is necessary and proportionate.

**11.2** PEMB will ensure Data Sharing Agreements are in place and Due diligence is carried out on third parties

**11.3 Data Processing Agreements (DPAs)** will be used where required.

## 12. International Data Transfers

**12.1** Personal data will not be transferred outside the UK unless:

- Adequacy regulations apply, or
- Appropriate safeguards (e.g. IDTA or SCCs) are in place

## 13. Confidentiality

**13.1** All staff and volunteers must maintain confidentiality.

**13.2** Confidential information must not be disclosed unless authorised, required by law and necessary to protect vital interests

**13.3** Confidentiality clauses will be included in contracts and volunteer agreements.

## 14. Data Retention and Disposal

**14.1** PEMB will follow a documented **Data Retention Schedule**.

**14.2** Personal data will:

- Not be kept longer than necessary
- Be securely destroyed when no longer required

**14.3** Disposal methods include:

- Shredding (paper)
- Secure deletion (electronic)

| Record Type | Retention Period | Reason for Retention | Action After Expiry |
|---|---|---|---|
| **Tenancy management records** | 6 years after tenancy ends | Limitation Act 1980 (legal claims) | Secure deletion |
| **Repairs and maintenance records** | 6 years | Legal/regulatory | Secure deletion |
| **Complaint records** | 6 years after closure | Housing Ombudsman guidance | Secure deletion |
| **Board/Director records** | 6 years after leaving | Governance and accountability | Secure deletion |
| **Minutes of meetings (Board, AGM)** | Permanent archive | Historical and legal reference | Archived securely |
| **Volunteer records** | 3 years after leaving | Safeguarding and accountability | Secure deletion |
| **Staff and employment records** | 6 years after employment ends | Employment law | Secure deletion |
| **Safeguarding concerns** | 10 years or longer if required | Safeguarding best practice | Reviewed, then securely deleted |
| **CCTV footage** | 30 days (unless required for investigation) | ICO guidance | Automatic or manual deletion |
| **Finance records (e.g. invoices)** | 6 years | HMRC requirements | Secure deletion |
| **Grant applications and reports** | 6 years | Funders' requirements and audit trail | Secure deletion |
| **Photos/media (with consent)** | Until consent withdrawn or 3 years | Marketing / community use | Secure deletion |
| **Website contact forms / enquiries** | 1 year | Responding to enquiries | Secure deletion |
| **Resident engagement surveys** | 2 years | Service improvement / reporting | Anonymised or securely deleted |

**Notes:**

- If a record is relevant to an ongoing dispute, complaint, legal claim or insurance matter, it may be retained beyond the stated period until resolution.
- Where data is anonymised (e.g. for statistical use), it may be retained indefinitely.
- All deletion or destruction of records will be logged where appropriate.

**Disposal Methods:**

- **Paper records**: Shredded and securely disposed of.
- **Electronic files**: Permanently deleted from devices and backups.

## 15. Records of Processing Activities (ROPA)

**15.1** PEMB will maintain records of:

- Data processing activities
- Categories of data
- Legal bases
- Data sharing

**15.2** This is required under Article 30 UK GDPR.

## 16. Data Protection Impact Assessments (DPIAs)

**16.1** DPIAs will be conducted where processing is likely to result in high risk, including:

- New systems
- Sensitive data processing
- Surveillance (e.g. CCTV)

## 17. Children's Data

**17.1** Where services involve children, PEMB will ensure:

- Appropriate lawful basis
- Parental/guardian consent where required
- Enhanced safeguards

## 18. Use of CCTV and Monitoring

**18.1** CCTV will be used only where necessary and proportionate.

**18.2** PEMB will:

- Display clear signage
- Follow ICO CCTV guidance
- Limit retention (as per schedule)

## 19. Training and Awareness

**19.1** All staff will receive:

- Mandatory data protection training
- Regular refresher training

**19.2** Training will be documented and monitored.

## 20. Roles and Responsibilities

**20.1 Data Protection Lead (DPL)**

*(Note: small organisations may not require a formal DPO)*

Responsible for:

- Compliance oversight
- Handling SARs and breaches
- Liaising with ICO

**20.2 Staff and Volunteers**

Responsible for following this policy; reporting incidents and protecting personal data

## 21. Governance and Accountability

**21.1** PEMB will demonstrate compliance through:

- Policies and procedures
- Training records
- Audit and monitoring

**21.2** The Board will oversee compliance.

## 22. Monitoring and Review

**22.1** This policy will be reviewed annually, or when legislation or operations change.

**22.2** Updates must be approved by the Board.

## 23. Monitoring and Review:

| | |
|---|---|
| **Approved by (full name):** | |
| **Role:** | |
| **Signature:** | |
| **Review date:** | |
| **Document version:** | |
| **Date read:** | |

## 24. Version control:

| Date | Notes | Staff Name |
|---|---|---|
| 28.04.2026 | Updated the policy to its latest standard as of 2026 | Gianna Schorno |
| | | |
| | | |
| | | |
| | | |