Data Protection Policy

1. Introduction

Peterborough Asylum and Refugee Association is committed to complying with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 to protect the privacy and personal data of all employees, volunteers, clients, and other individuals who interact with our services. This policy outlines the procedures that ensure personal data is handled lawfully, securely, and transparently.

2. Scope

This policy applies to all employees, volunteers, contractors, and third-party processors who have access to personal data handled by PARCA. It covers all personal data processed by the organisation, whether in electronic or paper form.

3. Lawful Bases for Processing

PARCA processes personal data under the following lawful bases:

- Consent: Where the data subject has given clear consent for their data to be processed for a specific purpose.
- Contract: Where processing is necessary for the performance of a contract with the data subject.
- Legal Obligation: Where processing is necessary to comply with a legal requirement (e.g., HMRC reporting).
- Legitimate Interests: Where processing is necessary for the legitimate interests of the organisation, provided that these interests do not override the rights and freedoms of the individual.

4. Data Subject Rights

Under GDPR, data subjects have the following rights:

- Right to Access: Individuals can request access to the personal data PARCA holds about them.
- Right to Rectification: Individuals can request corrections to inaccurate or incomplete data.
- Right to Erasure: Individuals can request the deletion of their data in certain circumstances.

- Right to Restrict Processing: Individuals can request a limitation on how their data is processed.
- Right to Data Portability: Individuals can request their data in a machine-readable format and transfer it to another service.
- Right to Object: Individuals can object to their data being used for certain purposes, including direct marketing.

Requests under these rights will be handled promptly and within the legal timeframes.

5. Data Security and Retention

PARCA is committed to ensuring the security of personal data by implementing appropriate technical and organisational measures. Employees must ensure that:

- Data is accurate, up-to-date, and processed only for its intended purpose.
- Data is stored securely, whether in electronic or paper form.
- Access to data is restricted to authorised personnel only.

5.1 Two-Factor Authentication (2FA)

- Two-Factor Authentication (2FA) is required for accessing all systems and databases that contain sensitive personal data, including employee records, client information, and financial data.
- 2FA combines something you know (e.g., a password) with something you have (e.g., a code sent to your mobile device or email). This extra layer of security is designed to ensure that only authorised users can access sensitive information.
- Employees must not disable or bypass 2FA. Any issues with the authentication process should be reported to the IT department or your line manager immediately.

5.2 Data Encryption

- All sensitive data stored electronically must be encrypted to protect it from unauthorised access.
- Data transmitted electronically must be encrypted, especially when being sent outside the organisation or across public networks.

5.3 Physical Security

- Data stored in physical form (e.g., paper records) must be stored securely in locked cabinets or rooms with restricted access.
- Sensitive information should not be left in public areas and should be disposed of securely when no longer required (e.g., shredding documents).

5.4 Retention Policy

- Data will be retained only for as long as necessary to fulfil its purpose and in accordance with PARCA's retention schedule. Once the data is no longer needed, it will be securely deleted or destroyed.

6. Reporting Data Breaches

Any employee who becomes aware of a data breach must report it to the Data Protection Officer (DPO) or their Line Manager immediately. In compliance with GDPR, PARCA will report any data breaches that pose a risk to individuals' rights and freedoms to the Information Commissioner's Office (ICO) within 72 hours. Affected individuals will be notified if the breach is likely to result in a high risk to their rights and freedoms.

7. International Data Transfers

Personal data will not be transferred outside the UK without appropriate safeguards in place, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or an adequacy decision by the UK government.

8. Data Processors and Third Parties

Any third-party processor handling personal data on behalf of PARCA must comply with GDPR through a data processing agreement. PARCA will ensure that these third parties provide sufficient guarantees to implement appropriate data protection measures.

9. Employee Responsibilities

Employees must:

- Ensure that personal data is handled in compliance with this policy.
- Follow secure data handling practices, including password protection and physical security measures.
- Report any concerns or breaches of data protection immediately to their Line Manager or DPO.

Failure to comply with this policy or GDPR may result in disciplinary action.

10. Employee Data

PARCA holds personal data about employees for the purposes of managing employment relationships. This data may include:

- References obtained during recruitment
- Details of terms of employment
- Payroll, tax and National Insurance information

- Performance information
- Details of grade and job duties
- Health and absence records
- Training records
- Emergency contact details

This data will only be shared with third parties where necessary (e.g., for payroll processing or government reporting) and in compliance with GDPR.

11. Data Protection Officer (DPO)

A designated Data Protection Officer (DPO) will oversee compliance with GDPR and act as the point of contact for data protection queries or concerns. The DPO will conduct regular reviews and audits of data processing activities to ensure ongoing compliance.

12. Training and Awareness

PARCA will provide regular training on data protection to all staff to ensure they are aware of their responsibilities under GDPR and DPA 2018. This training will be updated as necessary to reflect changes in legislation or internal procedures.

13. Policy Review

This policy will be reviewed annually or as necessary in response to changes in legislation, guidance, or operational practices.

Change Record

Date of Change:	Changed By:	Version	Comments:
20/12/2023	CEO	1.0	Policy approved by the Trustees
14/10/2024	CEO	1.1	Policy revised for clarity and legal compliance
14/12/2024	CEO	1.1	Review and approved by the trustees

Renewal date: 13/12/2025