Post Office Orphans Benevolent Institution
DATA PROTECTION POLICY

Date of last review:	29 April 2021	**Review period:**	**2 years**
Date of next review:	29 April 2023	**Owner:**	Chair of POOBI
Version:	0.7		

Data protection

1. INTRODUCTION

1.1. Post Office Orphans Benevolent Institution ("**POOBI**"), registered with the Financial Conduct Authority as a Friendly Society (No. 37-BEN) with Charitable Status, is the Data Controller for the purposes of the United Kingdom General Data Protection Regulation (the "**UK GDPR**").

1.2. POOBI collects and uses certain types of personal data of the following categories of individuals:

1.2.1. Staff;

1.2.2. Trustees and Officers;

1.2.3. Members/Subscribers;

1.2.4. Beneficiaries; including children and young people where the parent(s)/guardian(s) have given their consent;

1.2.5. Donors;

and other individuals who come into contact with POOBI.

1.3. POOBI processes this personal data to fulfil its charitable purposes of [helping Royal Mail Group & Royal Mail Ltd families with children who face hardship]. The processing is carried out for the following purposes:

1.3.1. To assess parents' or guardians' financial means for support of children;

1.3.2. To assess hardship from financial, health and others causes;

1.3.3. To fairly prioritise our resources, to contact, communicate and pay money;

1.3.4. To analyse our performance in serving the beneficiaries;

1.3.5. For audit and financial governance;

1.3.6. To comply with statutory and contractual obligations relating to employment;

1.3.7. To comply with statutory and other legal obligations relating to safeguarding.

1.4. This policy aims to ensure that personal data is processed lawfully, fairly, transparently and securely and in accordance with the UK GDPR the Data Protection Act 2018 (the "DPA"), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and other related legislation (together the "UK Data Protection and Privacy Laws"). It applies to all personal data held in electronic systems and structured manual files, for as long as the personal data remains in POOBI's control.

1.5. This policy will be updated as necessary to reflect any possible changes to the Charity's organisation, new processing activities, new regulatory guidance, best practice and any amendments made to the UK Data Protection and Privacy Laws, and shall be reviewed every 2 years.

1.6. All POOBI Employees and contractors are required to read and confirm that they understand this policy.

2. PERSONAL DATA

2.1. 'Personal data' means any information that identifies or is capable of identifying an individual. A sub-set of personal data known as 'special category personal data' relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

2.1.6. an individual's sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a person.

2.2. Special category data, as well as personal data relating to criminal convictions and offences is given special protection under the UK Data Protection and Privacy Laws, and POOBI complies with all additional legal requirements whenever this type of data is collected and used.

3. THE DATA PROTECTION PRINCIPLES

3.1. POOBI is committed to complying with the seven data protection principles laid down in the UK GDPR at all times. This means that POOBI will:

3.1.1. process personal data lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency");

3.1.2. process personal data only for the purposes for which it has been collected ("purpose limitation");

3.1.3. collect and process only personal data that is adequate, relevant and necessary in relation to the purpose(s) for which it has been collected ("data minimisation");

3.1.4. ensure accuracy of personal data and will keep it up to date ("accuracy");

3.1.5. ensure that personal data is not held longer than is necessary for the purposes for which it has been collected and is disposed of in a secure manner, in accordance with the Retention Policy, and that it has been held in accordance with the Retention Policy ("storage limitation");

3.1.6. ensure that appropriate security measures, as required under the UK GDPR, are in place to safeguard integrity and confidentiality of personal data processed by POOBI("security");

3.1.7. be responsible for and able to demonstrate compliance with all these principles above ("accountability").

3.2. POOBI has procedures for responding to individuals' requests, complaints and queries relating to personal data and is committed to ensuring that at all times, any person dealing with personal data

on its behalf, will facilitate the exercise of data subjects' rights (as explained in more detail in paragraphs 7 and 8 below).

3.3. POOBI will share personal data with third parties only when it is necessary and lawful to do so (as explained in more detail in paragraph 5 below).

3.4. POOBI will address and manage any personal data breaches and any breaches of the UK Data Protection and Privacy Laws in accordance with the procedure in sections 10 and 11 below.

4. LAWFUL BASIS FOR PROCESSING

4.1. POOBI will only process personal data if it is able to rely on one of the following lawful bases, pursuant to Article 6 of the GDPR:

4.1.1. the individual has given us their informed, unambiguous and free consent to the particular type of processing of their personal data; or

4.1.2. the processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps to enter into a contract with the individual, at their request; or

4.1.3. the processing is necessary for the performance of a legal obligation to which we are subject; or

4.1.4. the processing is necessary to protect the vital interests of the individual or another; or

4.1.5. the processing is necessary for a legitimate interest of POOBI or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned. More details of this are given in the Privacy Notice.

4.2. To the extent that POOBI is processing special category personal data, it will also satisfy an appropriate condition for processing in accordance with Article 9 of the UK GDPR and Schedule 1 of the DPA.

4.3. To the extent that POOBI is processing personal data relating to criminal convictions and offences or related security measures (criminal offence data), it will also comply with Article 10 of the UK GDPR and Schedule 1 of the DPA.

5. DISCLOSURE OF PERSONAL DATA

5.1. The following list includes the most usual reasons why POOBI might authorise disclosure of personal data to a third party:

5.1.1. to give a confidential reference relating to a current or former employee or Trustee or Officer;

5.1.2. where it is necessary for the prevention or detection of crime;

5.1.3. where it is necessary for the assessment of any tax or duty;

5.1.4. where it is necessary to exercise a right or comply with an obligation conferred or imposed by law upon us (other than an obligation imposed by contract)

5.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings) or any investigation by a statutory authority or regulator;

5.1.6. for the purpose of obtaining legal advice;

5.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

5.1.8. for audit of POOBI's financial and other processes by company auditors;

5.1.9. for payroll, HR, insurance and pension services;

5.1.10. for the provision of Health and Safety advice and support;

5.2. Where POOBI receives requests from third parties (i.e. those other than the data subject, POOBI and its employees) to disclose personal data it holds, such data will not be disclosed unless necessary to comply with legal obligation or otherwise lawful.

5.3. All requests for the disclosure of personal data must be sent to the Secretary to the Trustees, who will review and verify the identity of the requesting third party before deciding whether to make any disclosure.

5.4. We regularly need to disclose personal data to:

5.4.1. the Rowland Hill Fund (registered charity No. 207479) for processing of grants and bursaries for payments.

5.4.2. Royal Mail PLC for the purposes of assessing regular hardship cases and for liaison in order to make payments to beneficiaries.

6. SECURITY OF PERSONAL DATA

6.1. POOBI will take reasonable steps to ensure that members of staff, trustees and officers will only have access to personal data where it is necessary for them to carry out their duties. All staff, trustees and officers will be made aware of this Policy and their duties under the UK Data Protection and Privacy Laws. POOBI will take all reasonable steps to ensure that all personal data is held securely and is not accessible to unauthorised persons.

6.2. For further details as regards security of IT systems, please refer to the POOBI ICT Policy.

7. SUBJECT ACCESS REQUESTS

7.1. Any request for confirmation if POOBI processes requestor's personal data and for access to such data needs to be treated as a potential data subject access request. All personal data relating to the individual held in electronic or manual files forming part of a filing system, should be considered for disclosure.

7.2. As part of a subject access request, individuals are entitled to the following information:

7.2.1. whether personal data about him or her are being processed;

7.2.2. the purposes of the processing;

7.2.3. the categories of personal data concerned;

7.2.4. the recipients or categories of recipient to whom their personal data have been or will be disclosed;

7.2.5. the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;

7.2.6. the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;

7.2.7. the right to lodge a complaint with the Information Commissioner's Office;

7.2.8. where the personal data are not collected from the individual, any available information as to their source;

7.2.9. details of the safeguards in place for any transfers of their data to locations outside the UK/European Economic Area.

7.3. All requests received by POOBI should be forwarded to the Secretary to the Trustees at poobisecretary@royalmail.com without any delay and not later than within 2 working days of receipt. POOBI is required to deal with data subject access requests in full without delay and at the latest within one month of receipt, unless there are grounds to extend that period by further two months (see Article 12(3) of the UK GDPR).

7.4. Any individual, including a child or young person, may appoint another person to request access to their data. Where a child or young person lacks capacity to understand their rights and the implications of making a subject access request (e.g. due to their age or some other reason, such as special educational needs), a third party, such as a parent or carer can make a request on their behalf. The Secretary to the Trustees must, however, be satisfied that:

7.4.1. the child or young person lacks sufficient understanding; and

7.4.2. the request made on behalf of the child or young person is in their interests.

7.5. POOBI must verify the identity of an individual making the request. In the event that an individual appoints another person to make a subject access request on their behalf, POOBI must be satisfied that the individual making the request has authorisation of the individual to whom the request relates, which may involve obtaining written verification of the requestor's identity and authorisation.

7.6. Access to personal data may be restricted or refused in instances where an exemption under the DPA applies, for example, the relevant information is covered by legal advice privilege or information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). POOBI must decide whether to apply any potential exemption (seeking legal advice where appropriate), based on the circumstances of a particular request.

7.7. A data subject access request does not need to be made in writing – oral requests can be valid but to enable POOBI to deal with them appropriately, any oral requests should be clearly documented and the requestor should be encouraged to confirm their request in writing. POOBI may ask for any further information reasonably required to locate the information.

7.8. An individual only has the right to access their own personal data, and therefore care must be taken not to disclose the personal data of third parties where consent has not been given and where it would not be reasonable to do so without their consent. In such cases, POOBI might need to apply redaction or compile extracts of the requestor's personal data. Particular care must be taken in the case of any complaint or dispute to ensure that confidentiality and/or legal privilege are protected.

7.9. All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by Secretary to the Trustees (seeking legal advice where appropriate). Any disclosure can only take place after the response is approved by Secretary to the Trustees. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about the rights to complain to the Information Commissioner's Office (the ICO) and to bring a civil claim and all additional information required under the UK GDPR. It must be sent within one calendar month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR).

7.10. Where some data in a document needs to be redacted prior to disclosure, a copy of the full document and the altered document should be retained, with the reason for the redactions.

8. OTHER RIGHTS OF INDIVIDUALS

8.1. Other rights of individuals that POOBI needs to comply with include the right to:

8.1.1. object to processing;

8.1.2. rectification;

8.1.3. erasure

8.1.4. restrict processing; and

8.1.5. data portability.

8.2. These rights apply only in certain circumstances and are not absolute. Please ensure that you follow the approach set out in this policy to ensure that POOBI's response to data subjects' requests is compliant with the UK GDPR and the DPA.

8.3. **Right to object to processing (Article 21 of the UK GDPR)**

8.3.1. Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purpose (which

includes profiling to the extent that it is related to such direct marketing). This right is absolute and where such an objection is made personal data shall no longer be processed by POOBI for direct marketing purposes and should be included into POOBI's suppression list to prevent any future marketing communications to that person.

8.3.2. An individual also has the right to object to the processing of their personal data where their personal data is processed on the grounds of a task carried out in the public interest or the legitimate interests of POOBI or a third party (see paragraphs 4.1 above) and they do not believe that in their particular situation those grounds are made out.

8.3.3. Where such an objection is made, it must be sent to the Secretary to the Trustees without any delay and in any case within 2 working days of receipt, and the Secretary to the Trustees will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the information is required for the establishment, exercise or defence of legal proceedings.

8.3.4. The Secretary to the Trustees shall be responsible for notifying the individual of the outcome of their assessment within one calendar month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR), including informing them about their rights to complain to the ICO and to bring a civil claim.

8.4. **Right to rectification (Article 16 of the UK GDPR)**

8.4.1. An individual has the right to request the rectification of inaccurate data without undue delay and at the latest within one calendar month. Any request for rectification received by POOBI should be forwarded to the Secretary to the Trustees without any delay and in any case within 2 working days of receipt. Where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified. Any processing of the relevant personal data should be restricted until POOBI considers the request.

8.4.2. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be documented and notice of refusal should be provided to the individual within a month of receipt of the request (unless there are grounds to rely on the extension of time). Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about rights to complain to the ICO and to bring a civil claim. The individual shall be also given the option of a review under the complaints procedure and can complain directly to the Information Commissioner.

8.4.3. The individual must be notified within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR) about the outcome of their request.

8.5. **Right to erasure (Article 17 of the UK GDPR)**

8.5.1. Individuals have a right, in certain circumstances, to have their personal data permanently erased without undue delay. This right arises in the following circumstances:

8.5.1.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed; or

8.5.1.2. where consent is withdrawn and there is no other legal basis for the processing; or

8.5.1.3. where an objection has been raised under the right to object, and found to be legitimate; or

8.5.1.4. where personal data is being unlawfully processed; or

8.5.1.5. where there is a legal obligation on POOBI to delete.

8.5.2. The Secretary to the Trustees will determine the outcome of any request for erasure of personal data, and will balance the request against the exemptions provided for in the law. A response must be sent to the requestor within one calendar month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about their rights to complain to the ICO and to bring a civil claim. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, POOBI should make reasonable attempts to inform those controllers of the request.

8.6. **Right to restrict processing (Article 18 of the GDPR)**

8.6.1. In the following circumstances, individuals can have processing of their personal data restricted:

8.6.1.1. where the accuracy of data has been contested, during the period when POOBI is attempting to verify the accuracy of the data;

8.6.1.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

8.6.1.3. where data would normally be deleted, but the individual has requested that their personal data be kept for the purpose of the establishment, exercise or defence of a legal claim;

8.6.1.4. where there has been an objection to the processing, pending the outcome of any decision.

8.6.2. The Secretary to the Trustees will determine the outcome of any request. A response must be sent to the requestor within one calendar month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about individuals' rights to complain to the ICO and to bring a civil claim.

8.7. **Right to portability (Article 20 of the UK GDPR)**

8.7.1. In certain circumstances, if an individual wants to receive their personal data that they have provided to POOBI or have it sent to another organisation, they have a right to request that their personal data is provided in a structured, commonly used, and machine readable format. If a request for this is made, it should be forwarded to the Secretary to the Trustees without undue delay and in any case within 2 working days of receipt, and the Secretary to the Trustees will review and revert as necessary.

8.7.2. The Secretary to the Trustees will determine the outcome of any request. A response must be sent to the requestor within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about individuals' rights to complain to the ICO and to bring a civil claim.

9. PERSONAL DATA BREACHES

9.1. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Any identified or suspected personal data breaches shall be reported to the Secretary to the Trustees as soon as they are discovered. The Secretary to the Trustees shall consider any alleged breach and take appropriate steps.

9.2. Once **notified** of a suspected personal data breach, the Secretary to the Trustees shall assess:

9.2.1. the extent of the breach;

9.2.2. the risks to the data subjects arising out of the breach;

9.2.3. any security measures in place that will protect the personal data;

9.2.4. any measures that can be taken to contain the breach and to mitigate the risk to the individuals.

9.3. If following the assessment of a breach (the ICO's breach assessment tool may be used as part of the assessment process: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/),the Secretary to the Trustees concludes that the breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be notified to the ICO within 72 hours of the breach having come to the attention of POOBI. Any delay would need to be justified to the ICO.

9.4. A form for personal data breach reporting, published on the ICO's website (https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/) should be used to report personal data breach and the information provided to the ICO should include:

9.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

9.4.2. the contact point for any enquiries which shall usually be the Secretary to the Trustees, POOBI, Royal Mail, 185 Farringdon Road LONDON EC1A 1AA;

9.4.3. the likely consequences of the breach;

9.4.4. measures proposed or already taken to address the breach.

9.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Secretary to the Trustees shall notify data subjects of the breach without undue delay..

9.6. Notification to data subjects should describe in clear language the nature of the personal data breach and contain at least the following information:

9.6.1. the nature of the breach and its likely consequences;

9.6.2. who to contact with any questions;

9.6.3. measures taken or proposed to be taken to mitigate any risks and possible adverse effects of the personal data breach.

9.7. The Secretary to the Trustees shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the committee

of Trustees and Officers of POOBI and a decision made about implementation of those recommendations.

9.8. All personal data breaches, whether they are reportable to the ICO or not, will be recorded internally in POOBI's personal data breach log.

10. BREACHES OF THE UK DATA PROTECTION AND PRIVACY LAWS

10.1. Any potential breaches of the Data Protection and Privacy Laws, including a breach of any of the data protection principles, shall be reported to the Secretary to the Trustees as soon as they are discovered. The Secretary to the Trustees shall consider any alleged breach and take appropriate steps.

11. CONTACT

11.1. If anyone has any concerns or questions in relation to this policy they should contact the Secretary to the Trustees POOBI, Royal Mail, 185 Farringdon Road LONDON EC1A 1AA or at poobisecretary@royalmail.com