

POOBI Document retention (2021)

Date of last review:	29 April 2021	Review period:	2 Years
Date of next review:	29 April 2023	Owner:	Chair of POOBI
Version:	0.5		

1. INTRODUCTION

- 1.1. The main aim of this policy is to enable POOBI to manage our records effectively and in compliance with data protection law, namely: the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018") and other legal and regulatory requirements. As an organisation we collect, hold, store and create significant amounts of data and information. This policy explains our requirements to retain certain data and provides guidance on appropriate data disposal.
- 1.2. This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, [audio and video recordings and CCTV recordings]. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data". Only part of all data is covered in the Retention Schedule and this policy also explains how to treat day-to-day, disposable data.
- 1.3. This policy also covers data that is held by third parties on our behalf, for example cloud storage providers [or offsite records storage]. [It extends to data that belongs to us but is held by employees or volunteers on their personal devices.
- 1.4. POOBI is committed to the principles of data protection including the principle that personal data is only to be retained for as long as necessary for the purpose concerned (the storage limitation principle).
- 1.5. The table in the Appendix sets out the main categories of data that we hold, the length of time that we intend to hold them, and the reason for this.
- 1.6. This policy applies to all staff, trustees, volunteers and contractors engaged by POOBI. All such persons must understand and comply with this policy. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. Contractor's failure may lead to the termination of their contracts.
- 1.7. The Secretary to the Trustees is responsible for overseeing the implementation of this policy and for monitoring compliance. If you have any concerns or questions regarding retention of data or data disposal or need to report non-compliance, please contact the Secretary to the Trustees at poobisecretary@royalmail.com.

2. TYPES OF DATA

- 2.1. **Retention Schedule data.** Certain types of data, which are more important to us, are listed in the Retention Schedule in the Appendix. This may be because we have a legal requirement to retain such data, or because we may need it as evidence of our activities or transactions, or because it is otherwise important to the long-term running of our organisation. Please see the Appendix for information on retention periods for this type of data.
- 2.2. **Disposable data.** Disposable (day-to-day) data consists of data that serves only temporary purpose and is not a part of any formal or official record included in the Retention Schedule. Such data should be deleted or discarded by the user once it has served its temporary purpose (please see paragraph 4.4 below for more information on retention of this type of data). Examples of disposable data include:
 - duplicates of original documents that have not been annotated;
 - preliminary drafts of documents that do not represent significant steps or decisions in the preparation of an official record;

- manuals, training materials and other printed materials obtained from sources outside of our organisation and retained for reference purposes;
 - spam and junk mail and day-to-day emails that are no longer relevant to our organisation's needs.
- 2.3. **Personal data.** Both the Retention Schedule data and disposable data may contain personal data (i.e. data that identifies or is capable of identifying living individuals). Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it has been collected (principle of storage limitation). See paragraph 4 below for more information on retention periods for personal data.

3. PRINCIPLES OF DATA RETENTION

- 3.1. Through our data retention practices, we aim to meet the following commitments:
- comply with legal and regulatory requirements to retain data;
 - comply with our data protection obligations;
 - handle, store and dispose of data responsibly and securely; and
 - allocate appropriate resources and responsibilities to data retention, regularly monitor compliance with this policy and update this policy when required.

4. DOCUMENT RETENTION PERIODS

- 4.1. The Retention Schedule contained in the Appendix sets out the categories of data that we hold, the length of time that we need to retain them, and the reason for this.
- 4.2. Any data within the categories listed in the Retention Schedule, must be retained for the period assigned to the relevant category in the Retention Schedule. It must not be retained beyond that period, unless a valid business or legal reason calls for its continued retention (for example notice to preserve documents for contemplated litigation or another special situation outlined in paragraph 6 below).
- 4.3. Where personal data is listed in the Retention Schedule, we have considered the principle of storage limitation and balanced this against our requirements to retain the data.
- 4.4. The Retention Schedule does not set out retention periods for disposable data. Such data (which no longer has any business purpose or value to the organisation), should be securely disposed of. If data is not listed in the Retention Schedule, it is likely that it should be classed as disposable data. However, if you consider that there is an omission in the Retention Schedule, or if you are unsure whether to retain certain records, contact the Secretary to the Trustees, who will make decision.

5. STORAGE, BACK-UP AND DISPOSAL OF DATA

General

- 5.1. Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our operations during an emergency must be duplicated and/or backed up regularly [at least monthly] and back-up copies maintained off site.
- 5.2. When a document is at the end of its retention period, it should be dealt with in accordance with this policy. The Secretary to the Trustees is responsible for overseeing the process of identifying the data at the end of its retention period and its safe destruction.
- 5.3. If a document has reached the end of its stated retention period, but you are of the view that it should be retained for longer, please refer to the Secretary to the Trustees, who will decide

whether it should be retained and for how long. The reasons for extension and the new retention period should be documented.

- 5.4. It may be necessary to delete certain personal data before the end of the retention period in response to a data subject request for erasure. Such requests should be forwarded to the Secretary to the Trustees who will decide how to proceed.

Confidential data

- 5.5. The destruction of confidential data (confidential documents include financial records, employee-related records, ballots used to vote at trustee meetings and other documents containing commercially or otherwise sensitive information) must be conducted by shredding. Any documents that contain personal data should be treated as confidential. Confidential waste should be made available for collection in the confidential waste bins or sacks.
- 5.6. If confidential data is in an electronic format, please see section 5.8 (electronic data) below.

Non-confidential data

- 5.7. Non-confidential hard copy data (which does not contain any personal data) may be disposed of by recycling.

Electronic data

- 5.8. The deletion of electronic data must be overseen by the Secretary to the Trustees who will decide whether the relevant data should be deleted irretrievably, archived or, in cases where permanent deletion is temporarily impossible for technical reasons, 'put beyond use' (with appropriate safeguards in place and commitment for permanent deletion when it becomes possible).

Automatic deletion

- 5.9. Certain information will be automatically archived by the computer systems. Should you want to retrieve any information, or prevent this happening in a particular circumstance, please contact The Secretary to the Trustees.

What to consider when deciding whether to dispose of any data

- 5.10. When faced with a decision about deletion or disposal of data, you should comply with the Retention Schedule and if in doubt, consider the following:
 - 5.10.1. has the information come to the end of its useful life?
 - 5.10.2. is there a legal requirement or other justification to keep this data beyond the retention period? For example, would this data be likely to be needed in the case of any legal proceedings? (Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?) would the document be useful for the organisation as a precedent, learning document, or for performance management purposes?
 - 5.10.3. is the document of historic or statistical significance? If it includes personal data, is it possible to retain it in an anonymised form?
 - 5.10.4. are there any special circumstances set out in section 6 below?
- 5.11. If the decision is made to keep the document outside the Retention Schedule, this should be referred to The Secretary to the Trustees and reasons given.

6. SPECIAL CIRCUMSTANCES – PRESERVATION OF DOCUMENTS

- 6.1. The destruction of data must stop immediately if POOBI becomes aware that certain data may be relevant to current litigation or a dispute that could result in litigation, government investigation or audit. In addition, any routine data disposal procedures may need to be suspended as a result of a data subject request or in connection with a merger with another organisation or the replacement of our information technology systems.
- 6.2. In such circumstances, you must preserve and not delete, dispose, destroy, or alter such data (in whatever form), until the Secretary to the Trustees lifts the requirement for preservation.
- 6.3. If you believe the requirement for preservation may apply, please contact the Secretary to the Trustees.

7. OTHER RELEVANT POLICIES

- 7.1. This policy supplements and should be read in conjunction with our ICT Policy and Data Protection Policy.

APPENDIX – RETENTION SCHEDULE

DOCUMENT CATEGORY	RETENTION PERIOD	REASON
Constitutional		
Current rules of POOBI Friendly Society which are in force and previous amendments	Permanently	Legislation
Insurance		
???????		
Health & Safety		
General records	Minimum 3 years	Limitation Act 1980
Accident books/records and reports	3 years after last entry or end of investigation	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995
Charity Property		
No applicable		
Pension Records		
??????		
Tax and Finance		
Annual accounts and review (including transferred records on amalgamation)	Minimum 6 years Recommended: permanent record	CIO (General) Regulations 2012
Tax and accounting records	6 years from end of relevant tax year	Finance Act 1998 Taxes Management Act 1970
Banking records/receipts book/sales ledger	6 years from transaction	
Deed of covenant/Gift Aid declarations and correspondence re donations	6 years after last payment or 12 years if payments are outstanding or dispute over deed	As part of tax records
Legacies – correspondence and financial records	6 years after completion of estate administration	
Employees/Administration		
Payroll/Employee/Income Tax and NI records: P45; P6; PIID; P60 etc	6 years from end of current year	Taxes Management Act 1970 /IT (PAYE) Regulations
Maternity pay	3 years after the end of the tax year	Statutory Maternity Pay Regulations

Sick pay	3 years after the end of the tax year	Statutory Sick Pay (General) Regulations
HR files and training records	Maximum 6 years from end of employment	Limitation Act 1970 and Data Protection regulation
Job applications (CVs and related materials re unsuccessful applicants)	Recommended: 6-12 months from your notification of outcome of application	ICO Employment Practices Code (Recruitment & Selection) Disability Discrimination Act 1995 & Race Relations Act 1976
Pre-employment/volunteer vetting	6 months	ICO Employment Practice Code
Disclosure & Barring Service checks	Record only satisfactory/unsatisfactory result and delete other information	ICO Employment Practice Code
Volunteer records	Undertake assessment to decide on retention period taking account of risk (e.g. safeguarding re work with children or vulnerable adults)	Undertake assessment to decide on retention period taking account of risk (e.g. safeguarding re work with children or vulnerable adults)
Activity/Sector		
Grant applications		
Rising Stars, University Bursary and Regular Hardship Grant applications and tax forms	6 years plus current from last payment	Should any reference, complaint or enquiry arise and for financial accounting and taxation purposes
Unsuccessful applications	6 years plus current	Should any reference, complaint or enquiry arise