Central Finance Board of the Methodist Church and Epworth Investment Management Limited

Data Protection and Retention Policy

Version 2.0
Created May 23
Next review: May 2026 or earlier as per point 14.1

DATA PROTECTION AND RETENTION POLICY

1. Introduction

1.1 The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the European Economic Area (EEA). The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

It was adopted on 14 April 2016, and after a two-year transition period, became enforceable on 25 May 2018. The GDPR replaces the 1995 Data Protection Directive. Because the GDPR is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable. However the UK Government has produced the Data Protection Bill 2018 is necessary to make certain bits of GDPR work in the UK context and clarify and enhance certain aspects of GDPR. This policy takes account of all relevant legislation and Regulation.

1.2 The Central Finance Board of the Methodist Church (CFB) and Epworth Investment Management Limited (EIM) believe in treating people properly and looking after their data. We also seek to comply with the law in all that we do. A full description of how we use personal data can be found in our privacy notices which are published on the CFB and Epworth websites (www.cfbmethodistchurch.org.uk and www.epworthinvestment.co.uk).

1.3 We understand the relationship between Data Protection and confidentiality, and recognise that a clear policy on the confidentiality of Personal Data must work alongside and support Data Protection compliance.

1.4 The CFB and EIM take the protection of all personal information extremely seriously and are committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information.

1.5 We hold and process information about our current, past or prospective employees, job applicants, clients and unit holders and others who are defined as data subjects under GDPR. The CFB and EIM process personal information for a variety of reasons such as administering the payroll, recording information about investments and units held, monitoring attendance, and enabling references to be provided. Our Privacy notices for job applicants and staff contain full details of all processing and the legal bases for them. Where genuine consent is required we will ensure it is specifically asked for. The CFB and EIM may also be required by law or other regulations to collect and use certain types of personal information to comply with their needs.

1.6 EIM has duties under the Alternative Investment Fund Manager Directive (AIFMD). Specifically, the following articles from the directive apply and must be adhered to at all times:

Article 57 (2) AIFMs shall establish, implement and maintain systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question.

Article 58(2) AIFMs shall ensure a high standard of security during the electronic data processing and integrity and confidentiality of the recorded information, as appropriate.

Article 66(3) The records shall be maintained on a medium that allows the storage of information in a way accessible for future reference by the competent authorities, in such a form and manner that (a) the competent authorities are able to access them readily and reconstitute each stage of the processing of each transaction; (b) corrections or other amendments, and the contents of the records prior to such corrections and amendments, may be easily ascertained; (c) no other manipulation or alteration is possible.

2. Principles

2.1 All users of personal information within the CFB and EIM must comply with the six principles as laid out in GDPR. The Principles define how data can be legally processed. Processing includes obtaining, recording, holding or storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure and destruction.

2.2 The six principles state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Managing Data Protection

3.1 The CFB Council and Epworth Board recognise their overall legal responsibility for Data Protection compliance. We take the view that we are not required to have a formal Data

Protection Officer. Oversight of Data Protection is the responsibility of the Head of Change and Transformation, acting as our Data Protection Lead.

3.2 The role of the Data Protection Lead is:

- Reporting to the CFB Council and Epworth Board on Data Protection compliance
- Maintaining records that demonstrate how we comply with Data Protection
- Advising colleagues on Data Protection practice
- Ensuring that policies and procedures take Data Protection into account
- Ensuring that all relevant staff (including volunteers) receive Data Protection induction and regular training
- Reviewing contracts or contract amendments with Data Processors before they are signed
- Handling all requests from Data Subjects to exercise their Data Protection rights
- Being the point of contact for the Information Commissioner

3.3 All managers are responsible for Data Protection compliance within their teams and areas of responsibility, with advice and support from the Data Protection Lead.

4. Responsibilities

4.1. Staff and volunteers

4.1.1 All staff and volunteers have a responsibility to ensure they process personal information in accordance with the six Data Protection Principles and other requirements of GDPR including the requirements for the handling and processing of sensitive personal data

4.1.2 They are responsible for attending Data Protection training when invited

4.1.3 They must follow all organisational policies and procedures which underpin Data Protection.

4.1.4 They must pass any data subject access request to the Data Protection Lead when received without delay.

4.1.5 They are also responsible for reporting any breach, possible breach or near miss to their manager or the Data Protection Lead as soon as they become aware of it.

4.2 The Data Protection Lead will perform periodic audits to ensure compliance with this policy and to ensure that the notification to the Information Commissioner is kept up to date.

5. Data protection by design and by default

5.1 We incorporate Data Protection practice into all relevant processes and activities, and we consider the Data Protection implications of all new projects, activities and processes.

5.2 All major developments are reviewed by the Data Protection Lead. Managers are responsible for ensuring that Data Protection is taken into account when setting up or modifying routine processes.

6. Legal basis for processing

6.1 We carry out all our Processing of Personal Data under an appropriate Legal Basis, which is typically assessed as follows:

- Where the Processing is necessary for a contract that is normally the Legal Basis;
- Where the Processing is necessary under a legal obligation that is normally the Legal Basis;
- Where the Processing is necessary in the course of our routine activities our Legal Basis is normally legitimate interests, provided we have carried out and documented an appropriate assessment; and
- Where it is appropriate to offer the Data Subject a genuine choice, or where no other basis applies, our Legal Basis is normally consent.

6.2 We do not carry out any public functions, and we recognise that the vital interests Legal Basis is only to be used in the case of serious emergencies.

6.3 It is normally the responsibility of the team manager to assess the appropriate Legal Basis for the activities of their team and to carry out an assessment if required. Complex or potentially controversial cases may be referred to the Data Protection Lead or, exceptionally, to the CFB Council or Epworth Board.

7. Special categories of data

7.1 We obtain and process Special Category Data only where fully justified, including in the following situations:

- Where we wish to carry out diversity monitoring, with the explicit consent of the Data Subjects; and
- When processing staff sickness claims or claims under the PHI policy for staff.

8. Data subjects rights

8.1 All staff and volunteers are given guidance on how to respond when an individual asks to see information held about them or to exercise any of their other Data Protection rights.

8.2 All requests are forwarded to the Data Protection Lead, to ensure that our response is timely and complies with the relevant requirements.

9. Transfers abroad

9.1 We do not intentionally transfer Personal Data outside the UK, either directly or in the context of employing a Data Processor.

10. Collaboration with joint controllers

10.1 Whenever we collaborate with other organisations we establish at the outset whether we will be acting as joint Controllers of Personal Data. In that case we draw up a formal data sharing agreement, setting out the respective responsibilities of all parties involved in the collaboration.

11. Data Processors

11.1 Whenever we engage an external organisation to act as a Processor on our behalf the Data Protection Lead reviews any contractual terms and conditions offered, in order to establish that they meet Data Protection requirements. Where they do not, or where no standard terms and conditions are offered, we do not proceed until a compliant contract is agreed.

12. Data breaches

12.1 In the event of a Data Protection breach, possible breach or near miss, the Data Protection Lead, as a matter of priority, obtains all the necessary information and notifies the Information Commissioner – and any affected Data Subjects – if required. Whether or not the breach is reported, the Data Protection Lead investigates fully, proposes any necessary mitigating action or changes to procedure, and makes a report to the Board.

13. Document retention

13.1 The table below sets out the retention periods for various document types. These apply to both CFB and Epworth correspondence.

Reference	**Subject of record**	**Contents of record**	**When record must be made**	**Minimum retention period**
Records about Financial Promotions				
COBS 4.11	Financial Promotions	Financial Promotions communicated or approved by the Firm	When communicated or approved	5 years from the date of the Firm's communication or approval.
Records about Clients				
COBS 3.8.2R(2)	Client categorisation *NB: Where standard form documents are not used*	The categorisation and supporting information, evidence of dispatch of any notice and a copy of any agreement entered into in relation to categorisation	From the time of categorisation	5 years from the date of the Firm's communication or approval.
COBS 8.1.4R	Client agreements	Documents setting out rights and obligations of the Firm and the client	From date of the agreement	5 years after the cessation of the relationship with the client
Records about the Advisory Committee				

Reference	Subject of record	Contents of record	When record must be made	Minimum retention period
COLL 14.3.6R	Advisory Committee dealings	Dealings with the Advisory Committee including all relevant papers, minutes etc.	At the time of recording.	For a minimum period of 5 calendar years from the date of recording.
Records maintained by the Authorised Fund Manager				
COLL 6.6.6 R	Retention of documents	The Authorised manager and the scheme must make and retain such records as to comply with the rules of the COLL sourcebook and at all times be able to demonstrate that such compliance has been achieved. See below for further details:	At the time the records are created.	For a period of 6 years.
COLL 6.6.6 R	Scheme records	A daily record of the units in the scheme held, acquired or disposed of by the authorised fund manager including the classes of such units and the balance of any acquisitions and disposals.	At the time the records are created.	For a period of 6 years.
COLL 6.6.6 R and COLL 6.3.8R	Dilution calculations	Retain information about how it calculates and estimates dilution.	At the time the records are created .	For a period of 6 years.
COLL 6.6.6 R and COLL 6.3.8R	Dilution policy	Policy and method of determining the amount of any dilution levy or dilution adjustment.	At the time the records are created.	For a period of 6 years.
Records about Employees				

Reference	Subject of record	Contents of record	When record must be made	Minimum retention period
COBS 11.7.4R(3)	Personal transaction	Details of the personal transaction notified to the Firm	From date of notification	5 years
Records about the Firm				
COBS 2.3.17R (1)	Inducements	Each fee, commission or non-monetary benefit given	When benefit is given	5 years
SYSC 9.1.1R	Systems and controls	Details of the Firm's business and internal organisation	Ongoing	5 years from when a particular record was made
SYSC 10.1.6R	Conflict of interest	Details of the kinds of services and activities carried out by the Firm in which a conflict has arisen or may arise	Ongoing	5 years from when a particular record was made
SUP 17.4.3 & AIFMD Article 66(1)	Data retention	Data relating to transactions in financial instruments, including the identity of the client and information required under the money laundering directive	Ongoing	At least 5 years from when a particular record was made
AIFMD Article 66(2)	Data retention	Above records	On and after termination of the authorisation of EIM as an AIFM	At least 5 years from when the record was made
AIFMD Article 66(2)	Data transfer	Above records	Where EIM transfers its responsibilities as AIFM to another AIFM	Records must be made accessible to the new AIFM.
Financial records				

Reference	Subject of record	Contents of record	When record must be made	Minimum retention period
Companies Act/ Charities Act	Purchase invoices	Invoices, credit notes	On receipt	6 complete years from the end of the year in which the transaction was made. 10 years for capital invoices
Companies Act/ Charities Act	Sales invoices	Invoices, credit notes	On creation	6 complete years from the end of the year in which the transaction was made.
Companies Act/ Charities Act and HMRC	Petty cash records	Petty cash slips, receipts	On receipt	6 complete years from the end of the year in which the transaction was made.
Companies Act/ Charities Act and HMRC	Income/ monies received	Bank paying in counterfoils, bank statements, remittance advices, bank recs, cash book and sales ledger	On creation/ receipt	6 years from the end of the financial year in which the transaction was made.
Taxes Management Act	Payroll records	Payroll reports,	Payroll reports, notices of codings, P45s, P46s, P60's etc.	6 years plus the current year.
Commercial considerations	Capital expenditure	Successful quotes	On receipt	Permanently
Human resources records				
Limitations Act 1980	Staff files and training records	Contracts, HR files, Correspondence etc.	On receipt	6 years after employment ceases
DDA 1995 and RRA 1976	Job applications (unsuccessful candidates)	Application forms, interview notes etc.	On receipt/ creation	Up to a year
GDPR	Redundancy information	Details, calculations, notifications, correspondence etc.	On creation/ receipt	6 years after employment has ceased
Commercial	Organisation charts		On creation	Permanently

Reference	Subject of record	Contents of record	When record must be made	Minimum retention period
Building records				
Limitations Act 1960	Leases	Lease documentation	When created	15 years after expiry
Limitations Act 1960	Drawings and plans	Drawings, plans, certifications, consents H&S file etc.	When created	Permanently or until 6 years after building is disposed of
GDPR	Records of major refurbishment	As above	When created	13 years for action against contractors
	Personal injury claims	Correspondence etc.	When received	Generally claims commenced within 3 years of injury. (extended for industrial injury)
Insurance records				
GDPR	Policies		When received	3 years after lapse
GDPR	Claims	Correspondence etc.	When received	3 years after settlement
Employers Liability (compulsory Insurance) Regulations 1998	Employer liability certificates	Certificates	When received	40 years
GDPR	Accident reports	Reports, correspondence etc.	When created	3 years after settlement
Governance records				
GDPR	Minutes of meetings	Board, Council and committee minutes and meeting papers	When created	Permanently
GDPR	Annual accounts and annual review	Signed accounts and printed annual reviews	When created	Permanently
GDPR	Major agreements		When created/ signed	Permanently

14. Review of the policy

14.1 This policy will be reviewed once every three years and, if necessary, amended at other times to ensure continued compliance with GDPR, AIFMD and other relevant legal and compliance related obligations.