House of Commons Members Fund
Data Protection Policy (the "Policy")

Index

1 Who we are

This data protection policy has been prepared by the Board of Trustees ("the Trustees") of the House of Commons Members Fund ("the Fund").

As Trustees of the Fund, we hold certain personal information (known as "**Personal Data**") about Fund members and, where applicable, their dependants and beneficiaries. **Personal Data** is the information from which you can be identified and any personal information we hold or process in respect of you will be subject to certain protections

The Trustees are known as the "**Data Controller**" as we decide the purposes for and the means by which the **Personal Data** we collect and hold is **Processed**.

Owing to the nature of their role, the Fund actuary will be a joint **Data Controller** of **Fund Personal Data** alongside the Trustees.

2 Purpose of this Policy

Data Protection Legislation places obligations on organisations involved in the **Processing** of **Personal Data** about individuals. Both complying with the legislation, and being able to demonstrate compliance, are essential. Protecting Fund **Personal Data** also plays an essential role in ensuring the good governance of the Fund more generally.

This Policy sets out how we meet our obligations under **Data Protection Legislation**. The requirements of this Policy are supplemented by the Privacy Notice to which all members have access.

For ease of reference, key terms used in this Policy are defined in section 5.

3 Scope of this Policy

This Policy applies to the Trustees, all persons appointed as individual trustees from time to time and to the Secretary to the Trustees, together with all other employees of relevant bodies who provide support to the Fund and have access to **Fund Personal Data** (collectively referred to as the "**Relevant Parties**").

All **Fund Personal Data** collected by us electronically or in structured paper files (or which is intended to be in such a filing system) is covered by this Policy. This Policy sets out the Trustees' requirements relating to data protection and the legal conditions that must be satisfied in relation to the **Processing** of **Fund Personal Data**. However, this Policy is also subject to the general requirements of Data Protection Legislation.

Failure to comply with this Policy may also mean that Relevant Parties are in breach of their contractual commitments in respect of the Fund.

4 Responsibility for this Policy

The Trustees are responsible for ensuring that this Policy meets all applicable legal requirements and that all **Relevant Parties** comply with it. Any questions, exceptions to or breaches of this Policy should be referred to the Secretary to the Trustees.

Having considered the requirements of **Data Protection Legislation**, as well as the advice received from our legal advisers, we have concluded that we do not need to appoint a Data Protection Officer. If our circumstances or regulatory requirements change, we will review this decision with our legal advisers.

5 Meaning of key words / phrases used in this Policy

This Policy uses the following key words and phrases:

- **Data Controller** means any legal or natural person who alone, or jointly with others, determines the purposes for and the means by which Personal Data is Processed. For the purposes of this Policy, the Trustees are considered the Data Controller.
- **Data Subjects** are individuals on whom Personal Data is held and will include Fund members (both current and former), their dependants and beneficiaries (both actual and potential).
- **Data Processor** means any legal or natural person that Processes Personal Data on behalf of the Data Controller, for example, the Fund administrators.
- **Data Protection Legislation** means, as applicable, the United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018) and any legislation and/or regulation implementing or made pursuant to it , together with any law or regulation which amends, replaces, supplements or consolidates any of the foregoing from time to time.
- **UK GDPR** means the United Kingdom General Data Protection Regulation (UK GDPR)
- **ICO** means the Information Commissioner's Office, the UK regulatory body charged with ensuring compliance with Data Protection Legislation.
- **Personal Data** means any information (whether opinion or facts) relating to an identified or identifiable living person (or Data Subject). An identifiable living person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his/her identity. The fact that information is publicly available does not stop Data Protection Legislation applying to it.
- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Fund Personal Data.

- **Process / Processes / Processing / Processed** covers virtually anything done with Personal Data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination (or otherwise making available), or destruction.
- **Relevant Parties** has the meaning set out in section 3.
- **Fund Personal Data** means any Personal Data (including Special Categories of Personal Data) held:
    - in relation to members (both current and former), their dependants and beneficiaries (both actual and potential), including their names, postal addresses, email addresses, dates of birth, national insurance numbers, bank account and salary details, and all facts and opinions recorded about an individual; and
    - by the Trustees (or on our behalf) about those providing services and advice to the Fund (eg our Fund administrators, suppliers and advisers).
- **Special Categories of Personal Data (i.e. sensitive Personal Data)** is Fund Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

  For the Fund, **Special Categories of Personal Data** may be relevant when dealing with discretionary cases.
- **Third Parties** has the meaning set out in section 9.

6 Complying with the Data Protection Principles

We are committed to complying with our obligations under **Data Protection Legislation** whenever we, or someone acting on our behalf, are **Processing Fund Personal Data**. As **Data Controllers**, we must comply with the data protection principles set out in Appendix 1.

7 Transferring Fund Personal Data

Any transfers of **Fund Personal Data** will be carried out securely, whether externally to **Third Parties** such as Fund administrators, or internally between Trustees and **Relevant Parties**.

Before transferring **Fund Personal Data** (whether by email, post, fax or otherwise) whether internally or externally, **Relevant Parties** and **Third Parties**:

- should check that the information is being sent to the correct recipient.

- should consider asking another individual (namely, someone else who is authorised to have access to the **Fund Personal Data**) to check documents before they are sent. In particular, such checks should be carried out when transferring **Special Categories of Personal Data** or large volumes of **Fund Personal Data**.

- where required, should check the recipient's identity and/or that they have the authority to receive **Fund Personal Data**. This may involve carrying out checks to verify their identity, particularly if information is being released over the phone.

- should consider using secure methods of transmission, including password protection, encryption and "pseudonymisation" (i.e. making **Fund Personal Data** available on the basis that it can no longer be attributed to a specific individual without the use of additional information which is kept separately).

- where possible, should consider completely anonymising **Fund Personal Data**.

Email encryption should be used when large volumes of **Fund Personal Data** are sent by email (e.g. transfers of large spreadsheets of **Fund Personal Data**) or where **Fund Personal Data** that might be considered sensitive or confidential is sent by email.

8 International transfers

Data Protection Legislation restricts transfers of **Personal Data** outside of the European Economic Area (EEA), unless there is adequate protection for the **Personal Data** or prescribed steps have been taken to ensure that the **Personal Data** is protected. Regulations under section 17A of the DPA 2018 specify that all countries within the EEA are regarded as providing an adequate level of data protection. If personal data are transferred to a country outside the UK or EEA, the adequacy of that country and the organisations and systems processing the data is assessed to ensure that appropriate safeguards are in place.

We ensure that personal data is held in the UK and we intend to ensure that all aspects of our IT provision are UK (rather than EEA) based. We do not allow **Fund Personal Data** to be transferred outside of the EEA unless:

- it is transferred at the request and with the consent of the Fund member in relation to his/her own benefits

- it is required to fulfil a contractual obligation in respect of the member

Relevant Parties and **Third Parties** must inform us of any **Processing** of **Fund Personal Data** outside of the EEA.

9 The Third Parties we share Fund Personal Data with

As Trustees, we need to share **Fund Personal Data** with various **Third Parties** in order to help us to properly administer the Fund or, where relevant, because certain **Third Parties** have a justifiable interest in receiving **Fund Personal Data**. We are also under an obligation to share **Fund Personal Data** with certain regulatory authorities, such as HM Revenue & Customs.

We share **Fund Personal Data** with the following (which are referred to collectively in this Policy as "**Third Parties**"):

- our Fund secretary
- the third parties who are responsible for the day-to-day administration of the Fund on behalf of the Trustees
- the Fund's professional advisers, including the Fund actuary, auditor, investment consultants and lawyers
- the advisers and printers who help us prepare various communications we send to members
- the Bankers' Automated Clearing Service (BACS), or the Clearing House Automated Payment System (CHAPS) in order to pay benefits in the UK, or with Lloyds Bank (the Fund's banking providers) when benefits are being paid overseas.

10 Data sharing arrangements with Third Parties

Under **Data Protection Legislation**, the obligations that **Third Parties** are required to comply with (and the terms that need to be included in contracts) will depend upon whether they handle **Personal Data** as a **Data Controller** or a **Data Processor**. The distinction is important in determining who is primarily responsible for complying with legal requirements, and who can be liable for fines and compensation.

We may share **Fund Personal Data** with **Third Parties** in one of three ways, which will, in turn, dictate the nature of the agreement which will need to be entered between us.

10.1 Data Controller to independent Data Controller

Third Parties providing services to the Fund will be an independent **Data Controller** where they use the **Fund Personal Data** for purposes which are different to our own. Also, organisations or individuals under certain legal obligations to hold **Personal Data,** for example, accountants and insurers, might also be independent **Data Controllers** of **Fund Personal Data**.

There are no specific requirements under **Data Protection Legislation** regarding documenting data sharing arrangements between independent **Data Controllers**, as each separate **Data Controller** is responsible for complying with relevant requirements. However, when sharing **Fund Personal Data** with an independent **Data Controller** we will enter into an arrangement covering, as a minimum, the need for the independent **Data Controller** to comply with its obligations under **Data Protection Legislation** and, to the extent appropriate, limiting the use and onward transmission of **Fund Personal Data**.

10.2 Joint Data Controllers

Where two or more parties jointly determine the purposes and means of **Processing Personal Data** (using the same **Personal Data** for the same purposes), they will be joint **Data Controllers**. Each joint **Data Controller** has full liability resulting from a **Personal Data Breach**, unless one of the joint **Data Controllers** can show that it is not in any way responsible.

Owing to the nature of their role, the Fund actuary will be a joint **Data Controller** of **Fund Personal Data** alongside the Trustees.

Data Protection Legislation sets out specific requirements in relation to joint **Data Controllers**. Where we act alongside a joint **Data Controller** in relation to **Fund Personal Data**, we will do the following as a minimum:

- determine, in a transparent manner, how we are going to meet our respective responsibilities for complying with **Data Protection Legislation**, including meeting the information requirements to individuals (e.g. by a joint privacy notice) and dealing with individuals' rights (see section 11 below)
- put an arrangement in place to document the above
- make a summary of that arrangement available to members.

10.3 Data Controller to Data Processor

This is the most common arrangement that we enter with **Third Parties**. Our Fund administrators, secretary to the Trustees, legal advisers, benefit consultants, medical advisers and any other third party providers / advisers with whom the Trustees share Fund Personal Data as Data Processors will be **Data Processors**.

Under Data Protection Legislation, there must be a binding contract in place between a Data Controller and a Data Processor covering certain minimum requirements. We will ensure that all contracts with **Third Parties** who are **Data Processors** reflect the requirements under **Data Protection Legislation** (specifically Article 28 of the UK GDPR).

In addition, we will only use **Third Parties** as **Data Processors** where they provide sufficient guarantees that they have implemented appropriate technical and organisational measures so that the **Processing** of **Fund Personal Data** by them meets the requirements of **Data Protection Legislation** and the protection of individuals' rights.

11 Individuals' rights

Individuals' rights

We will always protect individuals' rights under **Data Protection Legislation** (to the extent applicable) including:

- **Right to information** – we provide our Fund members with access to information about how **Fund Personal Data** is Processed in our Privacy Notice (see section 2 above). This includes details of their various rights outlined in this section.

- **Rights of access (also known as a "Data Subject access request")** – **Data Subjects** have the right to see **Fund Personal Data** that is held about them and a right to have a copy provided to them, or someone else on their behalf, in a machine readable (namely, digital) format.

- **Right to rectification** – if at any point a **Data Subject** believes that the **Fund Personal Data** we hold about them is inaccurate, they can ask to have it corrected.

- **Right to restrict Processing** – **Data Subjects** can require us to limit the **Processing** of their **Fund Personal Data** in certain circumstances, for example, whilst a complaint about its accuracy is being resolved.

- **Right to be forgotten (or to erasure)** – **Data Subjects** can request that their **Fund Personal Data** is deleted altogether, although the Trustees can override this request in certain circumstances.

- **Right to object to Processing** – where we are relying on legitimate interests as a reason for **Processing**, **Data Subjects** can object to having their **Fund Personal Data Processed**, although we can override this objection and continue **Processing** that individual's **Fund Personal Data** where this is justified.

- **Withdrawing consent** – where we have relied on a **Data Subject**'s consent to **Process** their **Fund Personal Data** (for example, where a member has provided medical information to us as part of an early retirement application on grounds of ill-health), he/she can withdraw that consent at any time by notifying us. However, withdrawing consent will not affect the **Processing** of any **Fund Personal Data** which took place beforehand and it may be possible for us to continue **Processing** that individual's **Fund Personal Data** where this is justified.

- **Automated decisions** – a **Data Subject** also has a right not to be subject to the use of entirely automated decisions (including profiling linked to direct marketing) which produce legal effects or significantly affect the individuals. We do not currently use either of these in relation to Fund Personal Data and neither do any Third Parties.

- **Transfers outside of the EEA** – If Scheme personal data are transferred to a country outside of the EEA, the adequacy of that country and the organisations and systems processing the data is assessed to ensure that appropriate safeguards are in place. Where appropriate safeguards are in place and Fund Personal Data is being transferred outside of the EEA (or to an international organisation), we will tell members about the safeguards put in place, as well as providing details as to who to contact if they wish to obtain a copy or where copies of such safeguards are made available.

How we meet those rights

We inform **Data Subjects** of the above rights in the Privacy Notice. We will provide any required information or communication relating to the **Processing** of **Fund Personal Data** to a **Data Subject** in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

We will respond to requests without undue delay, and usually within one month of receipt of the request. Information will generally be provided to **Data Subjects** free of charge, although we can charge a reasonable fee in certain circumstances.

Requests by **Data Subjects** to see their records or to exercise any of their other rights under **Data Protection Legislation** should be made, in writing, to the Secretary to the Trustees who will take appropriate steps to deal with the issues raised.

Relevant Parties must:

- take care when entering information in free-text areas in any software systems as individuals to whom the information refers (such as Fund members) may see it at a later date. Information should only be entered which is appropriate and justifiable.
- forward any requests to see **Fund Personal Data** from any **Data Subjects**, or any other requests or complaints relating to the way in which their **Fund Personal Data** is processed, to the Secretary to the Trustees immediately. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt.

12 Accountability

Data Protection Legislation requires us to implement a wide range of measures to reduce the risk of a **Personal Data Breach** occurring and to demonstrate that we are taking data governance seriously. A description of some of the measures we have put in place to meet this requirement are set out in Appendix 2.

13 Personal Data Breach and lost devices

We must report a **Personal Data Breach** to the Information Commissioner's Office without undue delay (and where feasible within 72 hours), unless the breach is unlikely to result in a risk to the rights and freedoms of the individual and we can demonstrate this. We will also need to inform affected individuals where there is a high risk to their rights and freedoms.

In the event that any **Relevant Parties** and/or **Third Parties** become aware of a **Personal Data Breach**, it has been agreed that:

- they should notify the Secretary to the Trustees within 24 hours and provide as much information as possible (including the nature and the consequences of the **Personal Data Breach** and any measures taken or proposed to mitigate any adverse effects)

- the Secretary to the Trustees will investigate the cause of the **Personal Data Breach** and assess the risk to individuals, as well as establishing whether any action needs to be taken to recover any losses and to limit the damage caused by the **Personal Data Breach**
- where appropriate, the **ICO** and/or the police must be informed
- the **Personal Data Breach** must be recorded and, where applicable, the affected individuals informed
- the Secretary to the Trustees should also evaluate the effectiveness of the response to the **Personal Data Breach** and identify any amendments required to this Policy as a result, or to our, **Relevant Parties'** and **Third Parties'** technical or organisational measures in general.

Should an electronic device or any other storage media containing **Fund Personal Data** be lost or misplaced by the Trustees, please inform the Secretary to the Trustees as soon as possible.

14 Training and Guidance

All **Relevant Parties** should implement and ensure that all individuals handling **Fund Personal Data** receive appropriate training on **Data Protection Legislation** and security requirements, both when initially appointed or engaged and on an ongoing basis.

15 Audit

In order to demonstrate compliance with the data protection principles (see section 6) and other applicable requirements under **Data Protection Legislation**, we will undertake internal audits of our **Processing** activities from time to time. All **Relevant Parties** and **Third Parties** must cooperate with these audits.

16 Updates to this Policy

This Policy is the latest version as at01/02/2021. The information set out in this Policy may change and the Policy may need to be revised. It is also appropriate to review the Policy and the information, processes, decisions and records documented in it from time to time.

This Policy will be reviewed at appropriate intervals by us to ensure that it remains up-to-date and fit for purpose.

17 Who to contact about this Policy

For questions about this Policy, please contact Gurpreet Bassi, the Secretary to the Trustees at hcmf@parliament.uk or call 0207 219 1356.

Signed _____

Clive Betts
MP

Name _____

Chairman of the Trustees **Date 1 February 2021**

Appendix 1 – Complying with the Data Protection Principles

1 Lawfulness, fairness and transparency – Personal Data should be Processed lawfully, fairly and in a transparent manner

1.1 Lawful basis

We can only process **Fund Personal Data** where we have a lawful basis (or grounds) for doing so under **Data Protection Legislation**, and we must keep records of what that is or they are. The grounds for **Processing** which we rely on differ depending on the type of **Fund Personal Data**, namely, whether it is general **Fund Personal Data** (ie non-sensitive Personal Data) or **Special Categories of Personal Data**.

As we must have valid grounds for **Processing Fund Personal Data** at all times, and these grounds may change or cease to exist over time, we will keep the reasons outlined below under review.

General Fund Personal Data

The legal grounds for Processing which we generally rely on are:

- *Compliance with legal obligations* – to meet our trust law duties and responsibilities and/or legislative and regulatory requirements affecting the Fund.

- *Legitimate interests* – as the Trustees, we have a legitimate interest in **Processing Fund Personal Data** to ensure the proper administration of the Fund, and to enable us (and relevant **Third Parties**) to calculate and pay benefits.

  As required under the **Data Protection Legislation**, we will inform members of our legitimate interests. Although members have the right to object to **Processing** on these grounds (see section 11), we can override that objection where there are compelling reasons (e.g. because we need to process that **Fund Personal Data** in order to meet our legal obligation to pay benefits).

Special categories of Personal Data

Data Protection Legislation generally prohibits the **Processing** of **Special Categories Personal Data** unless certain conditions are met. The most relevant conditions for us to rely on are as follows:

- the member (dependant or beneficiary) having given their explicit consent to the **Processing** for one or more specific purposes. We will generally rely on consent when **Processing Special Categories of Personal Data.**

- the individual has him/herself made the **Special Categories of Personal Data** manifestly public.
- in order to establish, exercise or defend legal claims.

1.2 Fairness and transparency

To satisfy the requirement to be fair and transparent, **Relevant Parties** must communicate with members (and their dependants and beneficiaries) in a concise, transparent and intelligible manner, using clear and plain language that is easily understood.

We must tell members (and their dependants and beneficiaries) what **Fund Personal Data** is collected about them, how we intend to use it, who we share it with, if we intend to transfer it to another country outside of the European Economic Area ("EEA") (or to an international organisation), as well as letting them know how they can contact us with questions in order to exercise their rights (see section 11). – If Scheme personal data are transferred to a country outside of the EEA, the adequacy of that country and the organisations and systems processing the data is assessed to ensure that appropriate safeguards are in place. Where appropriate safeguards are in place and where **Fund Personal Data** is being transferred outside of the EEA (or to an international organisation), this includes letting members know what safeguards have been put in place, as well as providing details as to who to contact if they wish to obtain a copy or where copies of such safeguards are made available (see also section 8).

We will provide our Fund members with access to this information in our Privacy Notice.

If we need to ask for more **Fund Personal Data** or change how **Fund Personal Data** is **Processed**, we will consider if further information needs to be given to members.

2 Purpose limitation – Personal Data should be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes

Fund Personal Data must only be used for the purposes for which it was collected. The main purposes for which **Fund Personal Data** is likely to be collected by the Trustees (and **Relevant Parties / Third Parties** on our behalf) is to enable us to properly administer the Fund, and to calculate and pay benefits.

Relevant Parties should not use **Fund Personal Data** for any purposes which we have not told the members about, or which would not be obvious to that individual (or compatible with the original purposes for which it was collected). For example:

- **Relevant Parties** should not access **Fund Personal Data** for their own private purposes, or for friends or family. This is a serious issue and may be a criminal offence for which individuals can be prosecuted;
- **Relevant Parties** should only disclose **Fund Personal Data** with others within their own organisation where that person needs that information in order to perform their function in line with the specified purposes, or as otherwise permitted by us.

In determining whether a new purpose of **Processing** is compatible with the original purposes, we and the **Relevant Parties** will need to consider any link between the purposes, the context in which the **Fund Personal Data** has been collected, the nature of the **Fund Personal Data**, the possible consequences of the future **Processing** and any proposed safeguards.

3 Data minimisation – Personal Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed

Essentially, data minimisation means that we and **Relevant Parties** (and **Third Parties**) must only collect and use the **Personal Data** needed for the purposes we have identified (ie running the Fund properly, and calculating and paying benefits). We and **Relevant Parties** should continue to collect the **Fund Personal Data** we need but should keep data minimisation in mind when asking for information and sharing it, avoiding excess copying and/or sharing of **Fund Personal Data** with others (such as advisers) where it is not strictly necessary.

We will make regular checks on the relevance of **Fund Personal Data** being collected by **Relevant Parties** (and/or **Third Parties**) to ensure it continues to be proportionate to the purpose.

4 Accuracy – Personal Data should be accurate and, where necessary, kept up-to-date

High quality Fund Personal Data is fundamental to providing member benefits. We therefore encourage members to inform the Fund Administrator and/or the Secretary to the Trustees of any changes to their **Fund Personal Data** and have specifically drawn this right to their attention in the Privacy Notice. We will update, rectify or erase records (or ask that other **Relevant Parties** and **Third Parties** make the appropriate changes) to the extent required. In some cases, it may be necessary to request evidence to support a requested change.

Relevant Parties:

- will check the accuracy of **Fund Personal Data** upon being collected and at regular intervals;
- should not use **Fund Personal Data** they suspect might be out of date without confirming its accuracy;
- should take every reasonable step to ensure that inaccurate **Fund Personal Data** is corrected or securely deleted without delay;
- will update **Fund Personal Data** and relevant databases without delay if they are informed of a change in a member's (or dependant's or beneficiary's) **Fund Personal Data**; and

- will provide us with a regular report on how they are monitoring the accuracy of **Fund Personal Data**

5 Storage limitation – Personal Data should be kept in a form which allows an individual's identification for no longer than is necessary for the purposes for which the Personal Data is processed

To meet the requirements of both UK tax law, we must keep certain **Fund Personal Data** (for example, details about the date a member joins the Fund, their name and address, and details of benefits paid) for a minimum of 6 years.

However, given the long-term nature of the Fund, and the possibility of claims being brought in relation to the Fund many years after an individual has ceased to be a member, we consider that it is necessary to keep **Fund Personal Data** for at least the member's lifetime and for an appropriate period after that time, which reflects the potential for queries and complaints.

We will review **Fund Personal Data** on a regular basis. If we conclude that certain **Fund Personal Data** is no longer needed, that **Fund Personal Data** will generally be destroyed. We will also ensure that **Relevant Parties** and **Third Parties** regularly review **Fund Personal Data** held on our behalf and that appropriate steps are taken to delete, destroy or prevent access to **Fund Personal Data** that is no longer required. All such actions will be undertaken securely.

Where **Fund Personal Data** is used by **Relevant Parties** and/or **Third Parties** solely for the purposes of printing a communication, it will be retained by **Relevant Parties** and **Third Parties** for a maximum period of three months, after which it must be securely destroyed.

6 Integrity and confidentiality – Personal Data should be 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

Fund Personal Data will be kept and used securely from when it is first collected until its eventual destruction. We have therefore put in place appropriate technical or organisational measures to protect **Fund Personal Data** against unauthorised or unlawful **Processing**, and against accidental loss, destruction or damage, and to ensure that **Relevant Parties** and **Third Parties** do likewise. We will only transfer **Fund Personal Data** to **Third Parties** who have confirmed that they already have appropriate measures in place or who agree to put them in place.

The requirement to keep **Fund Personal Data** confidential and safe applies however information is held, whether on laptops or other portable devices, desktops, disks, USB sticks, as part of a database, in paper form or otherwise.

All **Relevant Parties** and **Third Parties** must observe the following requirements to keep **Fund Personal Data** confidential and secure:

6.1 Access

- Access to **Fund Personal Data** must only be given to **Relevant Parties** and **Third Parties** who have a genuine need to access such **Fund Personal Data** to carry out their duties to us. **Relevant Parties** and **Third Parties** must use secure filing cabinets, access controls and passwords to ensure this.
- Appropriate audit trails should be put in place to monitor access and amendments to records (for example, enabling an audit trail to be kept and accessed on computer systems). This is important to ensure that there is accountability for **Fund Personal Data**.
- Ensure that regular checks are undertaken to detect unauthorised or suspicious use of **Fund Personal Data**.

6.2 Physical security and storage of documents

- Where possible, **Relevant Parties** and **Third Parties** should keep desks clear of all documents containing **Fund Personal Data** at the end of each day. This information must be stored safely and securely in appropriate storage locations (e.g. filing cabinets / drawers / locked offices).
- Wherever possible, doors to areas where **Fund Personal Data** is stored and filing cabinets which contain **Fund Personal Data** should be locked and keys kept securely.
- Paper documents should be disposed of through confidential waste or by shredding.

6.3 Storage of electronic Fund Personal Data, off-site working and own devices

- All electronic **Fund Personal Data** should be stored on a secure network or on a computer which has appropriate security software installed. The security used on such systems should be regularly updated.
- **Fund Personal Data** relating to an individual is occasionally sent to that individual's personal email at the request of the member in question. This personal email address will be verified in the same way as an address verification.
- Unless we agree otherwise, or it is required in order to provide services to us, **Relevant Parties** and **Third Parties** should avoid unnecessary downloading or copying of **Special Categories of Personal Data** or large volumes of **Personal Data**. This applies to downloading or copying locally onto a database or any other device including laptops, desktops, mobile phones or other portable devices, USB sticks, CD-ROMs, databases, in paper form or otherwise.

- **Relevant Parties** and **Third Parties** who use electronic devices to process **Fund Personal Data** must do all that is reasonable to keep such devices, associated media and the **Fund Personal Data** contained therein secure at all times.

- **Fund Personal Data** held on USB sticks, CD-ROMs, floppy disks, or similar should be deleted when no longer required or, alternatively, such media should be physically destroyed.

6.4 Printing

- When printing **Fund Personal Data**, secure printing areas or locked printers should be used where available. Paperwork containing **Fund Personal Data** should be collected promptly and no unnecessary copies of **Fund Personal Data** should be printed.

Appendix 2 - Accountability

1 Records of Processing Activity

All organisations are required to keep records of all **Processing** activities, whether acting as a **Data Controller** or a **Data Processor**.

As **Data Controllers**, under Article 30 of the UK GDPR, the Trustees must keep written records of:

- their name and contact details and, where applicable, any joint **Data Controller**, and the **Data Controller**'s representative
- the data protection officer (where relevant)
- the purposes of the **Processing**
- a description of the categories of **Data Subjects** and of the categories of **Fund Personal Data**
- the categories of recipients to whom the **Fund Personal Data** have been or will be disclosed, including recipients in third countries (i.e. outside of the EEA) or international organisations
- where applicable, details of transfers of **Fund Personal Data** to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards in accordance with UK GDPR Article 49(1)
- where possible, the envisaged time limits for deleting the different categories of **Fund Personal Data**
- where possible, a general description of the technical and organisational security measures in place (as required by UK GDPR Article 32(1))

All **Relevant Parties** and **Third Parties** acting as a **Data Processor** on our behalf must keep a written record of all categories of **Processing** activities carried out on our behalf, containing:

- the name and contact details of the Trustees as **Data Controller** (and each **Data Controller**) and their name and contact details as **Data Processor**(s) and, where applicable, of our or their representative, and the data protection officer (if applicable)
- the categories of **Processing** carried out on our behalf (and each **Data Controller** generally)
- where applicable, transfers of **Fund Personal Data** to a third country or an international organisation, including the identification of that third country or

international organisation and the documentation of suitable safeguards in accordance with UK GDPR Article 49(1)

- where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the UK GDPR

2 Privacy by Design and by Default and Impact Assessment

We are required to implement technical and organisational measures to show we have considered and integrated data compliance measures into our **Processing** activities (known as "data protection by design and by default").

We commit to this by ensuring that, to the extent possible in respect of **Fund Personal Data**, we and other **Relevant Parties** and **Third Parties**:

- identify privacy risks at the outset of any project or before the implementation of a new product, system or service and plan for them accordingly
- in line with the data minimisation principle, pseudonymise, encrypt or anonymise **Fund Personal Data** where possible
- embed privacy into our technologies, operations and information architectures and consult all relevant stakeholders
- maintain the integrity and high standards of products and services, and
- strive to be transparent with individuals about what is done to protect their **Fund Personal Data.**

New products, systems or services developed by **Relevant Parties / Third Parties** should go through a privacy impact process to determine whether they affect the rights and freedoms of individuals. In some cases where "high risk" **Processing** is identified, a more thorough assessment (a "Data Protection Impact Assessment") will be required before it is commenced in accordance with the UK GDPR. The Privacy Impact Assessment will include a description of the **Processing** activities, the risks arising and measures adopted to mitigate those risks and, in particular, safeguards and security measures implemented to protect **Fund Personal Data** and to comply with the UK **GDPR** generally.