This **Joint Controller Agreement governing the obligations imposed by the Regulation (EU) 2016/679** made on [ ]

Between:

(1) **PMA Pension Fund**, registered in and established under the laws of United Kingdom whose registered address is at 96A Coleridge Street, Hove, East Sussex, BN3 5AA (the "Controller"); and

(2) **Workplace Pension Trustees Limited**, registered in and established under the laws of United Kingdom, Company Registration Number 08533061, whose registered address is at 5300 Lakeside, Cheadle, SK8 3GP (the "Controller")

Contents

BACKGROUND

(A) This Joint Controller Agreement has been agreed between the participating organisations identified as controllers under this Agreement.

(B) The Agreement covers access to personal data of service users for the purpose of managing a pension fund, and specific responsibilities and duties of each Controller will be described within this Agreement.

(C) The overall aim of this Agreement is to describe each Controllers responsibilities and sent out a consistent approach in protecting the confidentiality of personal data subject to the activities of the Controllers.

(D) Article 26 of the Regulation 2016/679 provides that the Controllers act in transparent manner and implement appropriate and necessary measures of processing that meet the requirements of the Regulation and ensure the protection of the rights of the data subjects as described in Article 13 and 14 of the Regulation.

(E) Both Controllers will designate a respective point of contact.

(F) In compliance with the above-mentioned provisions of the Regulation 2016/679 the Controllers wish to enter into this security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"**GDPR**" (General Data Protection Regulation) shall mean Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"**national law**" shall mean the law of the Member State in which the Processor is established;

"**personal information**" shall mean any information relating to an identifiable natural person ('data subject'); an identifiable person is one that can be identified, directly or indirectly, in particular by

reference to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic cultural or social identity of that person;

"processing personal data" shall mean obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data. This includes data manipulation if forms of organising and retrieving data; adaptation, alteration, or modification of the data; use of the information or data; transmitting the data and making data available; destroying, blocking, or erasing data.

"sub-contract" and "sub-contracting" shall mean the process by which wither party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted;

"technical and organisational security measures" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing; and

"DPIA" (Data Protection Impact Assessment) shall mean an assessment aimed at identifying risks to personal information.

"DPO" Data Protection officer.

2. CONSIDERATION

2.1 in consideration to Data Subjects, both Controllers engaging the services shall comply with the security, confidentiality and other obligations imposed under this Agreement.

3. PARTNERS TO THE AGREEMENT

3.1 This Agreement is between:

PMA Pension Fund and Workplace Pension Trustees Limited

3.2 The responsible directors detailed above have overall responsibility for the behaviour of their organisations and must ensure the Agreement is acted upon by relevant employees.

4. NATURE AND PURPOSE OF THE PROCESSING

4.1 The data processing is for the purpose of carrying out the duties of:

a) managing a pension fund in the capacity of a trustee

5. THE TYPE AND CATEGORIES OF PERSONAL DATA BEING PROCESSED

5.1 Personal Information shared for the purposes of this Agreement includes a range of information such as:

a) Name
b) Contact details
c) Date of birth
d) National Insurance Number
e) Financial information relating to the pensions
f) Employment details
g) Details of scheme beneficiaries
h) Information from ID verification agencies
i) Information from your existing or previous pension provider
j) Information from publically available sources such as Companies House
k) Insolvency or bankruptcy related data

5.2 We may come across and process data that is classed as Special categories data such as health records. We will ensure that member's consent is obtained when processing such data.

5.3 The processor does not carry out automated profiling of clients.

6. THE OBLIGATIONS AND RIGHTS OF THE DATA CONTROLLER

6.1 The Partners to this Agreement are "joint controllers" and will be separately responsible for the lawful processing of personal data, informing service users about the use of their personal data, the security of personal data, ensuring service users can exercise their rights, and applying any other relevant provision of the GDPR.

6.2 Both Data Controllers exercises the overall control over the data processing activities carried out by them.

6.3 The Data Controllers are responsible for:

a) Complying with the principles;
b) Honouring Data Subjects rights;
c) Ensuring the processing of the data is lawful;
d) Appointing a DPO;

e) Demonstrating compliance;
f) Managing a Joint Controller relationships;
g) Managing Data Processors, if appointed;
h) Record keeping;
i) Co-operation with the Supervisory Authorities;
j) Keeping personal information secure;
k) Ensuring transparency about Data Breaches;
l) Ensuring the Data Subject is notified with the relevant safeguards that are in place if the data is transferred into a third country.

7. INFORMING THE SERVICE USERS

7.1 The GDPR requires organisations to provide clear information to the Data Subjects, regarding the use of their personal data. Partners to the Agreement will discuss and agree on the best way to achieve this.

7.2 The Controllers will ensure that the relevant information is made available by most effective method, such as website, email or direct mail where appropriate.

8. CONDITIONS FOR CONSENT

8.1 The Legal basis of the processing under this Agreement is the carrying out Contractual Obligations in relation to the Establishing Trust Deed and Scheme Rules and related agreements that are necessary for compliant management of a pension scheme.

9. SUBJECT ACCESS REQUEST

9.1 The Data Controller must respond to Subject Access Requests from the Data Subjects within one month and provide information about:

a) the purpose of processing;
b) the categories of personal data held;
c) the recipients to whom the personal data has been disclosed;
d) the period for which the personal data will be kept and the criteria used in determining the period;
e) notification that the Data Subject has the right to request rectification of data kept;
f) notification that the Data Subject has the right to place a restriction to the processing of data subject to lawful restrictions;
g) notification that the Data Subject has the right for the data to be deleted, subject to any lawful restrictions;
h) the source of data, in the event that the data was not collected from the Data Subject.

9.2 The information requested will be provided in a simple and easily accessible format.

9.3 If further copies are requested, an administrative cost can be applied to the request to cover the cost of producing such copies.

9.4 The Subject Access Request will be carried out in a way so that they will not have a negative effect on the rights and freedoms of others.

10. RECORDS MANAGEMENT OF PROCESSING ACTIVITIES

10.1 Both Data Controllers shall maintain records of processing activities under their responsibility.

The Controllers need to keep the following records:

a) The details of the Controller, Processor (if one appointed), Representatives and the DPO;
b) The processing activities carried out;
c) Information relating to cross-border data transfers;
d) A description of security measures put in place to protect the data.

10.2 The records must be written and in electronic format where possible.

10.3 The records must be available for audit by the supervisory authority on request.

10.4 The records will be held and disposed of in line with the retention and disposal schedules as applicable for the services provided.

11. DATA PROTECTION IMPACT ASSESSMENTS

11.1 The Data Controllers ensure that DPIA has been undertaken to identify the key privacy risks and associated compliance and action plan has been developed. In the event of implementation of a new system or process that may have and adverse affect or carry a risk to personal data, the DPIA will be carried out by the Controllers.

12. APPOINTING A DPO

12.1 The UK Data Protection Bill 2018 Chapter 4. Chapter 69 puts further responsibilities on the UK based Data Controllers by requiring the appointment of a data protection officer as opposed to GDPR where the requirement is conditional.

12.2 The Data Protection officer is responsible for:

a) Providing information and advice in relation to GDPR processes and compliance;
b) Liaising with the Supervisory Authority;

c) Providing the Controller and their employees who are actively involved with processing the personal data with advice regarding how to implement and adhere to their obligations in the context of GDPR;
d) Monitor compliance with the GDPR, including raising awareness, assigning responsibilities and training staff involved with processing and related audits;
e) Provide advice in relation to DPIAs and monitor its performance pursuant to Art.33.

13. INFORMATION SECURITY

13.1 The Controllers agree that they shall maintain the personal data records and process the data with full audit trail information being retained in line with the required retention periods.

13.2 Each Controller shall notify the other as soon as practicable, latest after 7 working days, if they become aware of any unauthorised or unlawful processing, loss, destruction or damage to the data they hold.

13.3 Each Controller ensures that, the staff members responsible for the processing of personal data, have been adequately trained and are aware of the confidential nature of the data.

13.4 Each Controller will maintain and follow a documented process to ensure information security.

14. NOTIFYING OF PERSONAL DATA BREACH

14.1 Each Controller shall notify;
a) the other as soon as practicable, latest after 7 working days, if they become aware of any unauthorised or unlawful processing, loss, destruction or damage to the data they hold.
b) The Data Controller must notify the Supervisory Authority;
c) The Data Controller must make the Data Subjects aware of the breach if the breach has a potential negative effect on the data subjects.

14.2 The obligation to notify exists if:
a) The breach is likely to effect the rights and freedoms of data subjects;
b) There is a reputational risk, financial implication, loss of confidentiality, risk of discrimination, social and economic disadvantage that may fall on the data subject as a result of the breach;

14.3 Data breaches must be notified within 72 hours of the breach being discovered by downloading a form from the ICO website and sending it back to them.

14.4 Data Controller shall keep record of all data breaches containing the details and effects of the breach and action taken to rectify it.

15. APPOINTING A DATA PROCESSOR

15.1 The Joint Controllers shall not undertake any sub-contracting to Data Processors without the written consent from the other Controller.

15.2 If written consent is given, the same rules shall apply to the Data Processor as found in this Agreement.

15.3 Written and signed Controller and Processor Agreement will be required in the event of appointing the Data Processor.

16. TERM AND TERMINATION

16.1 This Agreement shall continue in full force and effect for so long as the processing personal data is required based on the Conditions of Consent (Paragraph 8).

16.2 In the event on one Controller no longer required to participate in the processing of the personal data, they have to notify the other controller of the reasons in writing. The exiting Controller remains responsible for retention of records for the time period as required by law.

17. COMPLAINTS

17.1 Each Controller has a formal Complaints procedure which the Data Subjects and partners to this Agreement can refer to and follow in the event of any complaints raising regarding the application of this Agreement.

18. GOVERNING LAW

18.1 This Agreement shall be governed by and construed in accordance with the laws of England and Wales.

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

This Agreement may be executed in any number of counterparts, and this has the same effect as if the signatures on the counterparts were on a single copy of this Agreement.

SIGNED on behalf of PMA Pension Fund

(Nominated Trustee signature)_____

PRINT NAME ANDREW EASTHAM

SIGNED on behalf of Workplace Pension Trustees Limited

(Trustee signature)_____

Stacy Lunnon