DATA PROTECTION POLICY

The World Markets Umbrella Fund plc (the "Fund")

7 March 2023

1. Purpose of Policy

This policy sets out details on how personal information ("**Personal Data**") relating to shareholders of the Fund ("**Shareholders**") or Personal Data relating to the directors, officers, employees and / or beneficial owner(s) of Shareholders that are not natural persons and Personal Data of directors and designated persons of the Fund and authorised signatories (all "**Data Subjects**") will be handled by the Fund and / or on its behalf by its third party service providers as and from 25 May 2018.

2. Data Protection Legislation

The Fund has obligations in respect of Personal Data in accordance with *inter alia*, the EU Data Protection Directive 95/46/EC, the Data Protection Acts 1988 to 2018, the ePrivacy Directive (2002/58/EC) and the General Data Protection Regulation (EU) 2016/679, together with any relevant associated guidance ("**Data Protection Legislation**").

Under Data Protection Legislation the Fund is a Controller, and accordingly the Fund must ensure that Personal Data processed by, or on behalf, of the Fund, is done so in accordance with the requirements set out in the Data Protection Legislation.

3. Delegation to Data Processors

The Fund delegates certain functions to the third party service providers set out below. As a result, the service providers process certain Personal Data on the Fund's behalf, and are accordingly deemed to be "**Processors**" within the meaning of Data Protection Legislation.

The Fund's Processors include:

- BNY Mellon Fund Services (Ireland) DAC (the "**Administrator**")
- City of London Investment Management Company Limited (the "**Investment Manager**") as investment manager and distributor
- Carne Global Financial Services Limited (the "**Secretary**")

In each instance, the Fund shall maintain a written agreement with the relevant Processor in respect of the processing of Personal Data, in accordance with the requirements of Data Protection Legislation. The Fund shall require, by virtue of confirmations provided in each agreement with the relevant Processor, that any obligations imposed on the Processor in respect of the processing of Personal Data are also applied by the Processor in their entirety to any sub-delegate of the Processor.

4. "Data Register" – Schedule of Processing Records

The Fund has conducted a data mapping exercise to ascertain the nature and type of Personal Data held by the Fund and by the relevant Processor. The Fund has documented this mapping exercise by means of a Schedule of Processing Records, i.e. a "Data Register" as required under Data Protection Legislation. The Data Register shall be maintained by the Fund and received on a periodic basis.

Personal Data means any data (or a combination of data) from which a living individual can be identified directly or indirectly. Personal Data can be factual or it can be an opinion about an individual, their actions and behaviour. As a result of the data mapping exercise, the Fund has determined that the Personal Data of investors held by it may include the following:

- Registered (or beneficial owner / related party) shareholder name
- Registered (or beneficial owner / related party) shareholder address
- Registered shareholder contact details – phone, fax, email
- Individual passport, drivers' license detail or similar
- Individual (or beneficial owner / related party) ID number – shareholder register account number, tax identifier code, social security identifier code or similar
- Individual bank account detail
- Transaction instruction and detail
- Individual signature

5. The Administrator as a Processor

The Fund has determined, as confirmed through its data mapping exercise that the Administrator processes the majority of Personal Data of the Fund and is considered to be the primary Processor of the Fund. The Fund has engaged, and shall continue to engage on an ongoing basis, with the Administrator in ensuring that the Administrator has, *inter alia*, implemented appropriate technical and organisational measures to ensure that its processing is compliant with the requirements of the Data Protection Legislation and that the rights of Data Subjects are protected. The Fund has entered into a written agreement with the Administrator to this effect. The Administrator has also been consulted in the preparation of the Data Register, and shall assist the Fund in maintaining the Data Register on an ongoing basis.

6. Data Protection Principles

There are a number of principles which must be satisfied when the Fund or its relevant Processor are handling, disclosing and storing Personal Data, including the following:

- ***Accountability:*** Notwithstanding that the Fund delegates functions to Processor, it is ultimately the Fund's responsibility to ensure that it complies with Data Protection Legislation. To ensure the Fund is accountable for its processing activities in accordance with the Data Protection Legislation, it has implemented compliance monitoring, data breach reporting, training and recording of processing procedures.

- ***Lawfulness, Fairness and Transparency:*** Processing of Personal Data may only be carried out when it is fair, lawful and transparent. This means that the Fund may only process Personal Data in accordance with Data Protection Legislation, in the manner in which it was described to the Data Subject, and shall inform the Data Subject of the purpose for which their Personal Data is being used. The Fund has provided a Data Protection Notice to all [Shareholders] and [directors [and designated persons] setting out the necessary information in accordance with the requirements of Data Protection Legislation.

- ***Purpose Limitation:*** Personal Data collected for one purpose cannot be used for a new, incompatible purpose. The Fund and the relevant Processor shall always seek to ensure that it does not process Personal Data in a way that is different to the manner for which Personal Data was originally collected.

- ***Data Minimisation:*** The Fund and the relevant Processor shall only hold as much Personal Data as is required, and any Personal Data held shall be specifically tied to a particular purpose, and limited only to that which is necessary to accomplish that purpose.

- ***Accuracy:*** Personal Data should be kept up to date, and the Fund and the relevant Processor should take every reasonable step to update or erase any inaccurate Personal Data by adopting appropriate checking procedures.

- ***Storage Limitation:*** The Fund and the relevant Processor should aim to ensure that all Personal Data held by it is active and necessary.

- ***Security/Integrity and Confidentiality:*** The Fund and the relevant Processor should always make sure that all Personal Data held by it is subject to a level of security that is appropriate for the potential risk, and processed in confidence with appropriate security procedures.

7. Data Subject Rights

Data Subjects have a number of rights in relation to their Personal Data, which are set out in the table below. The Fund shall comply with its obligations under Data Protection Legislation in respect of the exercise of these rights.

The cost incurred in facilitating the Data Subject's exercise of its rights shall be borne by the Fund, save where the Board determines that such a request is unjustified or excessive, whereby the cost may be charged to the relevant Data Subject.

Right	Further Information
Right of Access	A Data Subject has the right to request a copy of its Personal Data held by the Fund and to access the information which the Fund holds about it.
Right to Object	A Data Subject has the right to object at any time to the processing of its Personal Data where the Fund processes its Personal Data on the legal basis of pursuing the Fund's legitimate interests. If a Data Subject exercises this right, the Fund may no longer process their Personal Data unless the fund can demonstrate that it has an overriding legitimate interest to continue processing the Personal Data.
Right to Rectification	A Data Subject has the right to have any inaccurate Personal Data which the Fund holds about it updated or corrected.
Right to Erasure	In certain circumstances, a Data Subject may have its personal information deleted, for example if it exercises its right to object (see above) and the Fund does not have an overriding reason to process its Personal Data or if the Fund no longer requires Personal Data for the purposes as set out in the investor data protection notice.

Right to Restriction of Processing	A Data Subject has the right to ask the Fund to restrict processing Personal Data in certain cases, including if it believes that the Personal Data the Fund holds about it is inaccurate or the Fund's use of its information is unlawful. If a Data Subject validly exercise this right, the Fund will store Personal Data and will not carry out any other processing until the issue is resolved.
Right to Data Portability	A Data Subject may request the Fund to provide it with Personal Data which it has given the Fund in a structured, commonly used and machine-readable format and it may request the Fund to transmit Personal Data directly to another data controller where this is technically feasible. This right only arises where: (1) the Fund processes Personal Data with the Data Subject's consent or where it is necessary to perform the Fund's contract with the Data Subject; **and** (2**) the** processing is carried out by automated means.

If a Data Subject considers that the processing of Personal Data by the Fund or the relevant Processor infringes the provisions of relevant Data Protection Legislation, they may lodge a complaint with a supervisory authority in the EU Member State of their habitual residence, place of work, or in the place of an alleged infringement. In such circumstances, the Fund shall in all instances comply with its obligations under the Data Protection Legislation in connection with such complaints.

8. Data Protection Officer

The Fund, as a Controller, must determine whether, on the basis of the parameters set out in the Data Protection Legislation and relevant guidance, it is required to appoint a data protection officer ("**DPO**").

Article 37(1) of the GDPR states that it is mandatory for the following organisations to designate a DPO:

a) all public authorities and bodies, except the courts;

b) any Controller or Processor where the core activities of the Controller/Processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale; and

c) any Controller or Processor where the core activities of the Controller/Processor consist of processing special categories of sensitive personal data.

The Board has ascertained that the Fund is not a public authority or body, nor is its core activity the processing of special categories of sensitive personal data (for example, medical records). It therefore does not meet the requirements of categories (a) or (c) which obligate mandatory appointment of a DPO.

Furthermore, Data Protection Legislation makes it clear that "*systematic monitoring*" includes processing Personal Data as part of a "*general plan for data collection*", and "*large scale*" processing would be considered to include a high volume and wide range of Personal Data.

In light of this, and on the basis of the nature and scale of Personal Data processed by the Fund, the Board has determined that the Fund's core activity would not be considered to consist of "*regular and systematic*" monitoring of Data Subjects on a "*large scale*". Accordingly, the Fund would not be deemed to fall into category (b) above.

Therefore, the Board has determined that the Fund is not required to appoint a mandatory DPO under the Data Protection Legislation.

It is not anticipated that the nature and scale of Personal Data processed by the Fund shall change. However, this policy shall remain under annual review and it is open to the Board to revisit its analysis as to the necessity of appointing a DPO in the future.

9. Data Subject Requests

As set out above, Data Subjects whose Personal Data are processed by or on behalf of the Fund may make requests to the Fund in respect of their Personal Data, including for access, rectification, erasure or restriction of processing of their Personal Data.

Requests by Data Subjects shall be made to Josephine Kitcher at josephine.kitcher@citlon.co.uk

The Fund shall in all instances comply with its obligations under the Data Protection Legislation in adhering to applicable requests by Data Subjects regarding their Personal Data.

10. Data Protection Impact Assessments

The activities of the Fund would not currently necessitate conduct of a data protection impact assessment.

The activities of the Fund are not likely or anticipated to change over time, and accordingly it is not foreseen that the Fund will engage in any new types of processing of Personal Data, beyond that which is currently undertaken, that would necessitate a data protection impact assessment. However, should the Fund engage in any new processing activity requiring a data protection impact assessment, such an assessment would be carried out in accordance with requirements of Data Protection Legislation.

11. Reporting of Personal Data Breaches

The Fund's relevant Processor shall, in accordance with their respective written agreements with the Fund, inform the Board of notification of any Personal Data breaches.

The Fund shall report Personal Data breaches to the Data Protection Commission where the breach is likely to result in a risk to the rights and freedoms of natural persons, without undue delay (and in any event, within 72 hours of discovery of the breach). Where such a report is not made within 72 hours, the report, when made, shall be accompanied by an explanation regarding the delay.

The Investment Manager, on behalf of the Fund, shall maintain a database of all Personal Data breaches and related assessments, including details relevant to each Personal Data breach, the effects of the breach and any remedial action taken, if necessary.

12. International Transfer of Personal Data

The disclosure of Personal Data to third party recipients may involve the transfer of data to USA and India, and other jurisdictions outside the European Economic Area ("**EEA"**), which are not the subject of an adequacy decision by the EU Commission. Such countries may not be subject to equivalent data protection laws as countries within the EEA.

The Fund should ensure with the relevant Processor that any transfer of Personal Data to jurisdictions outside the EEA may only occur in accordance with the requirements of Data Protection Legislation.

13. Retention of Personal Data

The Fund shall retain Personal Data for as long as necessary or permitted in light of the purpose(s) for which it was obtained. The criteria used to determine the retention periods include:

- the length of the Fund's relationship with the Data Subject;
- whether there is a legal obligation to which the Fund is subject (such as retaining Personal Data obtained for the performance of AML and related checks, which will be kept for 5 years after termination of the relationship with the Data Subject); and
- whether retention is advisable in light of the Fund's legal position (such as with respect to statutes of limitations, litigation or regulatory investigations, in which case the Personal Data may be kept for up to 7 years).

14. Review of the Policy

This policy is subject to annual review by the Board of the Fund. The Board will undertake periodic training to ensure it keeps up-to-date with developments and best practice.

Date adopted: February 2019