ODEY WEALTH MANAGEMENT (UK) LIMITED

DATA PROTECTION POLICY

APRIL 2016

1 Policy statement

1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our business we may collect, store and process personal data about our staff, customers, clients, suppliers and other third parties, and we recognise the need to treat it in an appropriate and lawful manner.

1.2. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2 About this policy

2.1. The types of personal data that we may be required to handle include information about current, past and prospective staff, customers, clients, suppliers and others that we communicate with. The personal data, which may be held on paper, computer system, database or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.2. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3. This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5. The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is currently held by Kathryn Davies, Legal Department, 020 7208 1448, k.davies@odey.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

3 Definition of data protection terms

3.1. **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual or it can be an opinion about that person, their actions and behaviour. Examples of personal data include contact details, other personal information, photographs, expressions of opinion about an individual or indications as to our intentions about an individual.

3.4. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the

data controller of all personal data used in our business for our own commercial purposes where we have collected the data.

3.5. **Data users** are those of our staff members whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6. **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8. **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or for any alleged offence committed or alleged to have been committed by that person. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4 Data protection principles

4.1. Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

4.1.1. Processed fairly and lawfully.

4.1.2. Processed for limited purposes and in an appropriate way.

4.1.3. Adequate, relevant and not excessive for the purpose.

4.1.4. Accurate.

4.1.5. Not kept longer than necessary for the purpose.

4.1.6. Processed in line with data subjects' rights.

4.1.7. Secure.

4.1.8. Not transferred to people or organisations situated in countries without adequate protection.

5 Fair and lawful processing

5.1. The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include obtaining the data subject's consent to the processing, or notifying the subject that the processing is necessary for the performance of a contract or compliance with a regulatory or legal obligation to which the data controller is subject. When sensitive personal data is being processed, additional conditions must be met.

6 **Processing for limited purposes**

6.1. Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any new processing occurs.

6.2. We will process data about our clients for the purpose of managing their account, processing orders and keeping up to date records.

7 **Notifying data subjects**

7.1. If we collect personal data directly from data subjects, we will inform them about:

7.1.1. The purpose or purposes for which we intend to process that personal data.

7.1.2. The types of third parties, if any, with which we will share or to which we will disclose that personal data.

7.1.3. The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2.

7.3. All data subjects whose personal data we process are notified that we are the data controller with regard to that data, and we identify in our Data protection policy who the Data Protection Officer is.

8 **Adequate, relevant and non-excessive processing**

8.1. We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9 **Accurate data**

9.1. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date data.

10 **Timely processing**

10.1. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected with the exception being where we have been requested to keep the data for legal or regulatory purposes (e.g. in the event of a regulatory investigation). We will take all reasonable steps to destroy, or erase from our systems, all data which we deem is no longer required.

11 **Processing in line with data subject's rights**

11.1. We will process all personal data in line with data subjects' rights, in particular their right to:

11.1.1. Request access to any data held about them by a data controller (see also paragraph 15).

11.1.2. Prevent the processing of their data for direct-marketing purposes.

11.1.3. Ask to have inaccurate data amended (see also paragraph 9).

11.1.4. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12 **Data security**

12.1. We will use our best efforts to ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to personal data.

12.2. We will put in place procedures and technologies such as password protection and confidentiality agreements to maintain the security of personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they confirm to us in writing that they have adequate procedures in place themselves.

12.3. We will maintain data security by protecting and guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

12.3.1. **Confidentiality** means that only people who are authorised to use the data can access it.

12.3.2. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

12.3.3. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the company's central computer system or database instead of individual PCs.

12.4. Security procedures include:

12.4.1. **Entry controls.** Any unauthorised person seen in our office space without a member of staff should be reported immediately.

12.4.2. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

12.4.3. **Methods of disposal.** Paper documents should be shredded. Any data stored on computer systems, databases and digital devices should be physically destroyed when they are no longer required.

12.4.4. **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. All equipment requires a password to log on and PCs will automatically log out after 15 minutes if not used.

12.4.5. **IT.** We have implemented the necessary security systems such as firewalls, web filtering and anti-virus to secure and monitor our networks. We also carry out regular security testing on both staff and networks to increase security and awareness. Whilst we will use our best efforts to protect our computers and networks from viruses, spyware and other malicious codes, we cannot guarantee against unauthorised third parties hacking into our IT systems or using phishing, malware or cyberfraud techniques.

13 **Transferring personal data to a country outside the EEA**

13.1. We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

13.1.1. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

13.1.2. The data subject has given his consent.

13.1.3. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

13.1.4. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

13.1.5. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2. Subject to the requirements in paragraph 13.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14 **Disclosure and sharing of personal information**

14.1. We may share personal data we hold with any member of our Group, as defined in section 1159 of the UK Companies Act 2006.

14.2. We may also disclose personal data we hold to third parties:

14.2.1. In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

14.2.2. If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3. If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our staff, customers, clients or others.

14.4. However, we will not disclose your personal data to a third party without your consent unless we are not permitted to disclose the request to you (e.g. legal or regulatory investigations may prohibit disclosure of this fact) and we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

15 **Dealing with subject access requests**

15.1. Data subjects must make a formal request for information we hold about them. This must be made in writing and a fee is payable by the data subject for provision of this

information. Any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

15.2. We may record and monitor telephone conversations and reserve the right to use such recordings in any dispute that may arise.

15.3. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

15.3.1. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

15.3.2. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15.4. Any member of staff will refer to their line manager line manager or the Data Protection Officer for assistance in difficult situations. Members of staff should not be bullied into disclosing personal information.

16 Changes to this policy

16.1. We reserve the right to amend this policy at any time. The current policy will be made available to all data subjects upon request and will be displayed on our website: www.odeywealth.com