DATA PROTECTION POLICY

1. Introduction and purpose

1.1 Shaftesbury Capital PLC and certain of its subsidiary companies ("**Shaftesbury Capital**") collect, store and process a variety of Personal Data relating to individuals (including its employees, customers, tenants, shareholders, suppliers and other third parties) for business and legal reasons.

1.2 We are committed to the protection of Personal Data in all our business dealings and relationships. We will uphold all laws relevant to Personal Data, including those described within this Policy.

1.3 The purpose of this Policy is to set out:

1.3.1 How Shaftesbury Capital ("**we**", "**our**", "**us**", "**the Company**") handles Personal Data, and applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, customers, tenants, shareholders, suppliers and other third parties or any other Data Subject; and

1.3.2 What we expect from you in order for the Company to comply with applicable law.

1.4 This Policy must be complied with by all individuals working for Shaftesbury Capital at all levels, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), trainees, secondees, casual workers and agency staff (including in-house employees of outsourced service providers), volunteers, interns, consultants, agents or any other person associated with us (referred to in this Policy and its related guidelines as "**employees**", "**you**", "**your**"). You must read, understand and comply with this Policy and the related guidelines as relevant when Processing Personal Data on our behalf and complete training on its requirements.

1.5 This Policy and its related guidelines can be amended at any time.

2. Scope and compliance

2.1 This Policy is not intended as a definitive statement of the application of all applicable Data Protection and data privacy laws; instead it acts as a framework of best practice, setting out the key principles of Data Protection and data privacy that Shaftesbury Capital has adopted.

2.2 This Policy sets out the overarching compliance requirements and should be read with the related guidelines (adopted by Shaftesbury Capital from time to time) to which the requirements in this Policy apply. The related guidelines are available to help you interpret and act in accordance with this Policy. You must comply with the related guidelines to the same extent as you would this Policy.

2.3 Employees are responsible for ensuring that they comply with this Policy and the related guidelines. Line Managers must implement appropriate practices, processes and controls to ensure such compliance. Any breach of this Policy or the related guidelines governed by this Policy by any employee may result in disciplinary action, which could result in dismissal for gross misconduct.

2.4 The related Privacy Guidelines to this Policy comprise:

2.4.1 Data Breach
2.4.2 Data Protection Impact Assessments
2.4.3 Data Subject Access Rights
2.4.4 Data Retention
2.4.5 CCTV
2.4.6 Photography

2.5 The definitions used in this Policy and related guidelines are detailed in Section 4 below.

2.6 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR. The Privacy and Electronic Communications Regulations 2003 ("PECR"), which govern electronic marketing, now carry fines at the same level.

2.7 The DPM is responsible for overseeing this Policy and its related guidelines.

2.8 Please contact the DPM with any questions about the operation of this Policy, the related guidelines, the UK GDPR or if you have any concerns that this Policy or any of the related guidelines are not being or has not been followed**. In particular, you must always contact the DPM in the circumstances set out in Appendix 1.**

3. What is Data Protection Legislation?

3.1 The main source of data protection legislation in the UK is UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 ("**DPA 2018**"), each as amended by the Data (Use and Access) Act 2025. Together, this legislation governs the ways in which Personal Data relating to individuals can be collected and used. The legislation gives rights to individuals regarding their Personal Data and imposes obligations on persons (including companies) who Process such Personal Data, whether they do so in their own capacity or on behalf of others.

4. Definition of data protection terms

4.1 **Automated Decision-Making (ADM):** when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR permits Automated Decision-Making only with safeguards in place (information about the decision, the chance to make representations, human intervention and the right to contest the decision), and restricts it further where Sensitive Personal Data is involved.

4.2 **Automated Processing**: any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

4.3 **Consent**: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to

them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to our employees and Personal Data used in our business for our own commercial purposes.

4.4 **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

4.5 **Data Protection Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIAs should be conducted for all major system or business change programmes involving the Processing of Personal Data.

4.6 **Data Protection Manager (DPM):** the person with responsibility for data protection compliance, currently the Company Secretary.

4.7 **Explicit Consent**: consent which requires a very clear and specific statement (that is, not just action).

4.8 **ICO**: the Information Commission, the UK data protection regulator. It continues to be known as the ICO and was, until 30 September 2026, the Information Commissioner's Office.

4.9 **Personal Data**: means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about the Data Subject or an identifiable image e.g. from CCTV or a photograph.

4.10 **Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

4.11 **Privacy Guidelines**: the Company privacy guidelines provided to assist in interpreting and implementing this Policy as listed in paragraph 2.4.

4.12 **Privacy Notices or Privacy Policies**: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

4.13 **Processing or Process**: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

4.14 **Pseudonymisation or Pseudonymised**: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

4.15 **Related Policies**: the Company's disciplinary and IT Security policies.

4.16 **Sensitive Personal Data**: information revealing racial or ethnic origin, political or philosophical opinions religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life or orientation, biometric or genetic data used for identification purposes, and Personal Data relating to criminal offences, convictions or allegations. Sensitive Personal Data can only be processed under strict conditions, and are subject to additional legal requirements and therefore require additional care when handling.

4.17 **UK GDPR**: the UK version of the General Data Protection Regulation ((EU) 2016/679).

5. Personal Data Protection Principles

5.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).

b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).

d) Accurate and where necessary kept up to date (**Accuracy**).

e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

g) Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).

h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (**Data Subject's Rights and Requests**).

5.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**). To satisfy the Accountability requirement, Shaftesbury Capital maintains records which set out certain details about business processes which use Personal Data ("**Article 30 Records**"), which are reviewed and updated periodically. It is important that any changes to existing processing activities, or the introduction of new processing activities, are accurately reflected in the Article 30 Records.

6. Lawfulness, fairness, transparency

6.1 Lawfulness and fairness

6.1.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

6.1.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

6.1.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given his or her Consent;

b) the Processing is necessary for the performance of a contract with the Data Subject;

c) to meet our legal compliance obligations;

d) to protect the Data Subject's vital interests; or

e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices. Shaftesbury Capital provides Data Subjects with appropriate Privacy Notices.

6.1.4 You must identify and document the legal ground being relied on for each Processing activity.

6.1.5 Sensitive Data is generally only processed by HR. Employees outside of HR are advised not to ask for or to process Sensitive Data without seeking prior approval of the DPM. Where Sensitive Data is Processed, in addition to a lawful bases outlined in section 6.1.3, a further condition must be met. A list of the lawful bases and further conditions for Processing Sensitive Data is available in Appendix 2 sections 2 and 3.

6.2 **Consent**

6.2.1 A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR as outlined in 6.1.3 above, which include Consent. Examples of Shaftesbury Capital's activities that will require consent from Data Subjects include e-marketing and photography featuring individuals.

6.2.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.2.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly actioned. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.2.4 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

6.2.5 You will need to evidence the Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

6.3 Transparency (notifying data subjects)

6.3.1 The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.3.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data. All of Shaftesbury Capital's online or paper forms collecting Personal Data must include the Fair Processing Notice or state where this can be viewed online.

6.3.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must discuss with the DPM to ensure that the Data Subject is provided with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7. Purpose limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. The privacy notice issued to the Data Subject sets out the purposes for which Personal Data will be processed.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained (as set out in the privacy notice issued) unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

8. Data minimisation

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to

the purposes for which it is Processed. For example, when requesting background information in relation to a new residential tenancy, the Company should only collect categories of Personal Data which are necessary to assess the suitability of that prospective tenant, such as their ability to pay rent, rather than detailed information about their personal life.

8.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data and you should not hold Personal Data on a "just in case" basis for use in the future without having a clear idea of what that future purpose might be. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's Data Retention Guidance Note.

9. Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data when collected and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 The Company will maintain retention policies and procedures to ensure Personal Data is deleted a reasonable time after the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable. For example, previous employees of Shaftesbury Capital would expect the Company to retain their Personal Data for a period of time after they have left the business as legally required or so that an employment reference could be provided. However, the Personal Data retained should only be processed as necessary to meet these legal requirements rather than remain available for general processing. To achieve this, such Personal Data can be archived or access limited only to the specific information a specific business function requires.

10.5 You will ensure Data Subjects are informed of the period for which data is stored and how

that period is determined in any applicable Privacy Notice.

11. Security integrity and confidentiality

11.1 Protecting personal data

11.1.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.1.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.1.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who comply with the required policies and procedures and have put adequate measures in place, as (see Section 21.3 below).

11.1.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.1.5 Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

11.1.6 Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

11.1.7 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

11.1.8 You must comply with the prevailing IT Security Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

11.2 Reporting a personal data breach

11.2.1 The UK GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. The notification must be made without undue delay and, where feasible, within 72 hours of the Company becoming aware of the breach.

11.2.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11.2.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM or the General Counsel. You should preserve all evidence relating to the potential Personal Data Breach.

12. Transfer data outside the UK

12.1 The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

12.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

a) the UK has issued regulations confirming that the country to which we transfer the Personal Data provides a standard of protection for Data Subjects that is not materially lower than in the UK;

b) appropriate safeguards (as per Article 46 of the UK GDPR) are in place such as binding corporate rules (UK BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, and a transfer risk assessment has been completed. Please speak to the DPM if this is required;

c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

13. Data subject's rights and requests

13.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Data Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances (e.g. where the Personal Data is no longer needed for the purposes for which it was collected, but it is needed to establish of defend legal claims);

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) have safeguards applied to significant decisions based solely on Automated Processing, including profiling (ADM), such as human intervention and the right to contest the decision;

j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

k) make a complaint to us or to the ICO; and

l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 The DPM may ask you to verify the identity of an individual requesting data under any of the rights listed above (and must not disclose Personal Data to third parties without proper authorisation).

13.3 You must immediately forward any Data Subject request or complaint you receive to the DPM to comply with the company's Data Subject Access Rights Guidance Note.

14. Accountability

14.1 Under the UK GDPR, the Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles and must be able to demonstrate, compliance with the data protection principles.

14.2 Accordingly, the Company will ensure that it has adequate resources and controls in place to ensure and to document UK GDPR compliance including:

14.2.1 designating a suitably qualified DPM;

14.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects or when implementing major system or business change programmes involving the processing of personal data, as per the Data Protection Impact Assessment Guidance Note;

14.2.3 keeping accurate Article 30 records, ensuring they are updated regularly;

14.2.4 integrating data protection into internal documents including this Policy, Related Policies, Privacy Guidelines, Privacy Notices; and

14.2.5 regularly training employees on the UK GDPR, this Policy, and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company will maintain a record of training attendance by employees.

14.2.6 conducting periodic reviews and audits to assess compliance, to demonstrate compliance improvement effort.

15. Record keeping

15.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

15.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

15.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPM, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

16. Training and audit

16.1 We will ensure all employees have undergone adequate training to enable them to comply with data privacy laws. We will also regularly test and undertake periodic audits of our systems and processes to assess compliance.

16.2 You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

17. Privacy by design and Data Protection Impact Assessment (DPIA)

17.1 We are required to implement Privacy by Design measures when Processing Personal Data. This means considering privacy at the initial design stages and throughout the development process for any proposal that will involve the Processing of personal data and implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

17.2 Examples of privacy friendly approaches include anonymising data so that it is not possible to single out the information relating to a certain individual (Data Subject) or pseudonymising data, which still relates to specific individuals, but replaces key identifiers (names, national insurance numbers etc.) with pseudonmyns (such as a sequential or random number for each data entry) so that it is not possible to identify an individual from the data itself.

17.3 We are also required to conduct DPIAs in respect of any Processing that is likely to result in a high risk to the rights and freedoms of individuals. You should conduct a DPIA (and discuss your findings with the DPM) when implementing major system or business change programmes involving the Processing of Personal Data including:

17.3.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

17.3.2 Automated Processing including profiling and ADM;

17.3.3 large scale Processing of Sensitive Data; and

17.3.4 large scale, systematic monitoring of a publicly accessible area.

17.4 The Data Protection Impact Assessment Guidance Note contains screening questions which can provide an indication as to whether a DPIA is required. A template DPIA is also included in the Data Protection Impact Assessment Guidance Note.

18. Automated Processing (including profiling) and Automated Decision-making (ADM)

18.1 ADM is when a decision is made based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. We do not permit ADM unless this has been approved by the Chief Executive following consultation with the DPM, and any ADM must comply with the requirements of the UK GDPR.

18.2 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

19. Children

19.1 As children may be less aware of the risks involved in data processing, we must take particular care when collecting or processing their personal data.

19.2 Compliance and fairness must be central to any processing of children's personal data and if you are considering marketing to children you must take into account their reduced ability to recognise and critically assess the purposes and potential consequences of the processing.

19.3 Where children's data is processed, we must provide them with a privacy notice that is written clearly using age-appropriate language.

19.4 Children have the same rights over their personal data as adults, including a right for their personal data to be erased. This is particularly relevant where consent to processing was provided by an individual when they were a child.

19.5 Due to the increased sensitivities around processing of children's personal data, you must consult with the DPM if you are considering undertaking any work which would involve this.

20. Direct marketing

20.1 Specific rules and privacy laws (in particular PECR) apply to marketing communications, such as marketing emails.

20.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. All marketing opt ins must be freely given, meaning that:

a) tick boxes must not be pre-ticked

b) opt ins must not be bundled with other consents

c) acceptance of a free service must not be contingent on agreeing to receive marketing information.

20.3 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

20.4 [You must comply with the requirements on direct marketing included within the Photography Guidance Note.]

21. Sharing personal data

21.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Any transfer of Personal Data to a third party, including data hosting, will make the third party a Data Processor, as Processing includes the holding of data.

21.2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

21.3 You may only share the Personal Data we hold with third parties, such as our suppliers if:

21.3.1 they have a need to know the information for the purposes of providing the contracted services;

21.3.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

21.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

21.3.4 the transfer complies with any applicable cross border transfer restrictions; and

21.3.5 a fully executed written contract that contains UK GDPR-compliant clauses relating to the Processing of Personal Data has been obtained.

22. Changes to this Policy

22.1 Shaftesbury Capital reserves the right to change this Policy and its related guidelines at any time.

APPENDIX 1: WHEN YOU SHOULD CONTACT THE DATA PROTECTION MANAGER

1. If there has been a Personal Data Breach (Section 11.2)

2. If you receive a Data Subject Access Request (section 13);

3. If you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see Section 6);

4. If you need to rely on Consent and/or need to capture Explicit Consent (see Section 6.2);

5. If you need to draft Privacy Notices or Fair Processing Notices (see Section 6.3);

6. If you are unsure about the retention period for the Personal Data being Processed (see Section 10);

7. If you are unsure about what security or other measures you need to implement to protect Personal Data (see Section 11);

8. If you are unsure on what basis to transfer Personal Data outside the UK (see Section 12);

9. If you receive a more complex request by a Data Subject to change their details;

10. Whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Section 17) or plan to use Personal Data for purposes other than what it was collected for;

11. If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section 18);

12. If you need help complying with applicable law when carrying out direct marketing activities (see Section 20); or

13. If you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section 21).

APPENDIX 2 LAWFUL BASES FOR PROCESSING PERSONAL DATA & SENSITIVE PERSONAL DATA

1. In order to process Personal Data lawfully, you must identify a lawful basis or "condition" before you can process Personal Data.

2. All processing of Personal Data must be justified by reference to one of a number of lawful grounds or "conditions" for processing, as set out in Article 6(1) of UK GDPR. The legal bases or "conditions" listed in Article 6(1) of UK GDPR include:
    a) where it is necessary to perform a contract

    b) where it is necessary to comply with a legal obligation

    c) if you have a genuine and legitimate reason, unless this is overweighed by harm to an individual's rights and interests

    d) if you have obtained the individual's (i.e. Data Subject's) consent

    e) where it is necessary to protect someone's life;

    f) where it is required to carry out a public/official task; or
    g) where it is necessary for a recognised legitimate interest specified in the UK GDPR, such as preventing crime, safeguarding vulnerable individuals or responding to emergencies (please speak to the DPM before relying on this)

3. In addition, all processing of Sensitive Data must be justified by reference to one of a number of conditions/grounds for processing, as set out in Article 9(2) and Article 10 of the UK GDPR and as set out in more detail in the DPA 2018. In general, processing of Sensitive Data may take place:
    a) where the data subject has given explicit consent;

    b) where the processing is necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;

    c) where the processing is necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;

    d) where the processing relates to the personal data which are manifestly made public by the data subject;

    e) where the processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;

    f) where the processing is necessary for reasons of substantial public interest on the basis of UK law (see Schedule 1 to the DPA 2018), proportionate to the aim pursued and with appropriate safeguards;

    g) where the processing is necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

    h) where the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices;

or

i) where the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.