Data Protection Policy

1 Scope

We are committed not only to the letter of the law, but also to the spirit of the law and place high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom we deal.

We are not required by law to appoint a Data Protection Officer, however, Mr Peter James, is responsible for our compliance with the General Data Protection Regulations and matters arising there from, including administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

This Policy sets out our obligations in respect of how we process personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), now known as UK GDPR, the Data Protection Act 2018, and any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

The policy also details our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by our employees, agents, contractors, or other parties working on our behalf.

2 Definitions

Consent	The consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them
Data Controller	The natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, we are a data controller of all personal data relating to personal data provided to us in connection with the provision of our services and our commercial purposes.
Data Processor	A natural or legal person or organisation which processes personal data on behalf of a data controller
Data Subject	A living, identified, or identifiable natural person about whom the Company holds personal data
EEA	The European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway
Joint-data controller	Two or more data controllers that jointly determine the purpose and means of the processing of the same personal data
Personal Data	Any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier

	such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
Processing	Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data

3 Compliance With This Policy

All Directors and Managers are responsible for ensuring that all employees, agents, contractors, or other parties working on our behalf, comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy or to Data Protection Law should be referred to Mr Peter James, Director, in the first instance and, should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed

b) if consent is being relied upon in order to collect, hold, and/or process personal data

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data

d) if any new or amended privacy notices or similar privacy-related documentation are required

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests)

f) if a personal data breach (suspected or actual) has occurred

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors)

i) if personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment

k) when personal data is to be used for purposes different to those for which it was originally collected

l) if any automated processing, including profiling or automated decision-making, is to be carried out

m) if any assistance is required in complying with the law applicable to direct marketing, including the Privacy in Electronic Communications Regulations (PECR)

4 The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. As a Data Controller, we are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed

d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject

f) 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

5 The Rights of Data Subjects

The UK GDPR sets out the following key rights applicable to data subjects:

a) The right to be informed

b) the right of access

c) the right to rectification

d) the right to erasure (also known as the 'right to be forgotten'). This right is subordinate to our regulatory obligation to retain data, for example as required by HM Revenue & Customs, or in respect of clients, claims and complaints for the duration of the policy plus 6 years

e) the right to restrict processing

f) the right to data portability

g) the right to object

h) rights with respect to automated decision-making and profiling.

6 Lawful, Fair, and Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject

d) the processing is necessary to protect the vital interests of the data subject or of another natural person

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

We acknowledge that in order to process special category personal data (also known as "sensitive personal data"), we must meet one of the following conditions:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social

security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject)

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

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects

e) the processing relates to personal data which is manifestly made public by the data subject

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity

g) the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy)

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

7 Consent

When we are required to rely upon consent as our lawful basis for processing, for example marketing activities, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject

7.5 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that we can demonstrate our compliance with consent requirements

8 Specified, Explicit, and Legitimate Purposes

8.1 We collect and process the personal data set out in this Policy. This includes:

a) personal data collected directly from data subjects and

b) personal data obtained from third parties

8.2 We only collect, process, and hold personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the UK GDPR)

8.3 Data subjects are kept informed at all times of the purpose or purposes for which We use their personal data. Please refer to Part 15 for more information on keeping data subjects informed

9 Adequate, Relevant, and Limited Data Processing

9.1 We only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 24, below

9.2 Employees, agents, contractors, or other parties working on our behalf may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected

9.3 Employees, agents, contractors, or other parties working on our behalf may process personal data only when the performance of their job duties requires it. Personal data held by us cannot be processed for any unrelated reasons

10 Accuracy of Data and Keeping Data Up-to-Date

10.1 At all times, we will ensure that all personal data collected, processed, and held by us is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below

10.2 The accuracy of personal data shall be checked when it is collected. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate

11 Data Retention

11.1 We will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed and our

regulatory requirements to do so

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay

11.3 Details of our approach to data retention, including retention periods for specific personal data types held by us are available in our Data Retention Policy

12 Secure Processing

12.1 We shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes

13 Accountability and Record-Keeping

13.1 Peter James, Director, is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines

13.2 We follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information)

13.3 All employees, agents, contractors, or other parties working on our behalf shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

13.4 We regularly review our data protection compliance

13.5 We maintain written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

13.5.1 the name and details of the Company, who is responsible for data protection and all applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared)

13.5.2 the purposes for which we collect, hold, and process personal data

13.5.3 Our legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data

13.5.4 details of the categories of personal data collected, held, and processed by Us, and the categories of data subject to which that personal data relates

13.5.5 details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards

13.5.6 details of how long personal data will be retained by Us (please refer to our Data Retention Policy)

13.5.7 details of personal data storage, including location(s)

13.5.8 detailed descriptions of all technical and organisational measures taken by Us to ensure the security of personal data

14 Data Protection Impact Assessments and Privacy by Design

14.1 In accordance with the privacy by design principles, we shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects

14.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing

b) the state of the art of all relevant technical and organisational measures to be taken

c) the cost of implementing such measures

d) the risks posed to data subjects and to Us, including their likelihood and severity

14.3 Data Protection Impact Assessments shall be overseen by Peter James and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed

b) the purpose(s) for which personal data is to be used

c) Our objectives

d) how personal data is to be used

e) the parties (internal and/or external) who are to be consulted

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed

g) risks posed to data subjects

h) risks posed both within our business and to Us

i) proposed measures to minimise and handle identified risks

15 Keeping Data Subjects Informed

15.1 We acknowledge the requirement for us to provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained

15.2 The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and those responsible for data protection within the business

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 24 of this Policy) and the lawful basis justifying that collection and processing

c) where applicable, the legitimate interests upon which we are justifying its collection and processing of the personal data

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed

e) where the personal data is to be transferred to one or more third parties, details of those parties

f) where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see Part 31 of this Policy for further details)

g) details of applicable data retention periods

h) details of the data subject's rights under the UK GDPR

i) details of the data subject's right to withdraw their consent to Us processing their personal data at any time

j) details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR)

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

16 Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which we hold about them, what we are doing with that personal data, and why

16.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to Peter James, Director.

16.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed

16.4 All SARs received shall be handled by Peter James, Director.

16.5 We will not charge a fee for the handling of normal SARs. However, we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive

17 Rectification of Personal Data

17.1 Data subjects have the right to require Us to rectify any of their personal data that is inaccurate or incomplete

17.2 We shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing us of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed

17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data

18 Erasure of Personal Data

18.1 Data subjects have the right to request that we erase the personal data we hold about them in the following circumstances:

a) it is no longer necessary for Us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed

b) the data subject wishes to withdraw their consent to Us holding and processing their personal data

c) the data subject objects to Us holding and processing their personal data (and there is no overriding legitimate interest to allow Us to continue doing so) (see Part 21 of this Policy for further details concerning the right to object)

d) the personal data has been processed unlawfully

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation

18.2 The above notwithstanding, it is our regulatory obligation to retain client and accounting information for a minimum of 6 years by HMRC. This retention period overrides the right of erasure under the UK GDPR

18.3 For all other data, unless we have reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed

18.4 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so)

19 Restriction of Personal Data Processing

19.1 Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so)

20 Data Portability

20.1 We process personal data using automated means using recognised insurance quotation and client relationship management software, in addition to other recognised software providers such as Windows and Microsoft Office programs

20.2 Where data subjects have given their consent to Us to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between Us and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers)

20.3 To facilitate the right of data portability, we shall make available all applicable personal data to data subjects in a universally acceptable format

20.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller

20.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed

21 Objections to Personal Data Processing

21.1 Data subjects have the right to object the processing of their personal data based on legitimate interests, for direct marketing

21.2 Where a data subject objects to the processing of their personal data based on its legitimate interests, we shall cease such processing immediately, unless we can demonstrate that Our legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims

21.3 Where a data subject objects to the processing of their personal data for direct marketing purposes, we will cease such processing promptly

22 Automated Processing, Automated Decision-Making, and Profiling

22.1 We do not use automated processing, automated decision-making or undertake any profiling activities

23 Direct Marketing

23.1 We are subject to the rules or the General Data Protection Regulations and the Privacy in Electronic Communications Regulations when marketing our products and services

23.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) We may wish to send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from Us

23.3 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity

23.4 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with

24 Personal Data Collected, Held, and Processed

24.1 We collect, process and store only data necessary for the provision of insurance quotations and for the incepting and ongoing performance of insurance contracts

24.2 This will include personal data such as age, address, occupation and may include Special Category Data such as medical conditions and criminal conviction

24.3 Additional data may be obtained and shared as part of the performance of a contract of insurance, for example, in the event of a claim or complaint

24.4 We will retain data for no longer than is necessary. Please refer to our Data Retention Policy

25 Data Security - Transferring Personal Data and Communications

We shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

25.1 All emails containing personal data must be encrypted.

26 Data Security - Storage

It is our policy to ensure that the following measures are taken with respect to the storage of personal data:

26.1 All electronic copies of personal data should be stored securely using passwords and data encryption

26.2 All personal data stored electronically is backed up to the Cloud

26.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise, without the formal written approval of Peter James, Director., and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary

26.4 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken)

27 Data Security - Disposal

27.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to Our Data Retention Policy.

28 Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

28.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on Our behalf requires access to any personal data that they do not already have access to, such access should be formally requested from Peter James, Director.

28.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of Peter James, Director.

28.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time

28.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it

28.5 Where personal data held by Us is used for marketing purposes, it shall be the responsibility of Peter James, Director, to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS

29 Data Security - IT Security

We ensure that the following measures are taken with respect to IT and information security:

29.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols

29.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords

29.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. It is the responsibility of our IT department to install any and all security-related updates promptly after they are released by the software manufacturer/provider

29.4 No software may be installed on any Company-owned computer or device without the prior approval of Peter James, Director

30 Organisational Measures

We shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

30.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy

30.2 Only employees, agents, contractors, or other parties working on Our behalf that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company

30.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data

30.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so

30.5 All employees, agents, contractors, or other parties working on Our behalf handling personal data will be appropriately supervised

30.6 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise

30.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed

30.8 All personal data held by Us shall be reviewed periodically, as set out in the Company's Data Retention Policy

30.9 The performance of those employees, agents, contractors, or other parties working on Our behalf handling personal data shall be regularly evaluated and reviewed

30.10 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract

30.11 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law

30.12 Where any agent, contractor or other party working on Our behalf handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

31 Transferring Personal Data to a Country Outside the EEA

31.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

31.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

31.2.1 the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data

31.2.2 the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

31.2.3 the transfer is made with the informed and explicit consent of the relevant data subject(s)

31.2.4 the transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject)

31.2.5 the transfer is necessary for important public interest reasons

31.2.6 the transfer is necessary for the conduct of legal claims

31.2.7 the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

31.2.8 the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

32 Data Breach Notification

32.1 All personal data breaches must be reported immediately to Peter James, Director

32.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained

32.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), Peter James, Director must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it

32.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 32.3) to the rights and freedoms of data subjects, Peter James, Director, must ensure that all affected data subjects are informed of the breach directly and without undue delay

32.5 Data breach notifications shall include the following information:

32.5.1 The categories and approximate number of data subjects concerned

32.5.2 The categories and approximate number of personal data records concerned

32.5.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained)

32.5.4 The likely consequences of the breach

32.5.5 Details of the measures taken, or proposed to be taken, by Us to address the breach including, where appropriate, measures to mitigate its possible adverse effects

33 Implementation of Policy

33.1 This Policy shall be deemed effective as of Peter James, Director and replaces all previous Data Protection Policies in circulation within the firm.

33.2 This Policy and matters arising from it are reviewed annually and are the responsibility of Peter James, Director.