SMOKE VENT SYSTEMS LIMITED
DATA PROTECTION POLICY

1. Introduction

1.1 This Policy sets out the obligations of the Company regarding data protection and the rights of "data subjects" (such as customers) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

1.2 The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); the definition of "identified or identifiable natural person" is such broad terms that it covers almost every individual with whom the Company might have a relationship with, including, customers, individual named persons in a business even though the business itself might be limited company, and employees. The reference to "data subject" in this Policy therefore includes all such individuals, including employees.

1.3 This Policy sets out our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out below must be followed at all times by the Company, its employees, agents, contractors, and other parties working on our behalf.

1.4 We are committed not only to the letter of the law but also to its spirit, and we 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.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR that sets out a set of principles with which any party handling personal data must comply. In summary, all personal data must be:

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

2.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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

2.4 accurate and, where necessary, kept up to date;

2.5 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; and

2.6 processed in a manner that ensures appropriate security of the personal data.

3. The Rights of Data Subjects

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

3.1 the right to be informed;

3.2 the right of access;

3.3 the right to rectification;

3.4 the right to erasure (i.e. the 'right to be forgotten');

3.5 the right to restrict processing;

3.6 the right to data portability;

3.7 the right to object; and

3.8 rights with respect to automated decision-making and profiling.

4. Lawful, Fair, and Transparent Data Processing

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

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

4.1.2 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 with them;

4.1.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 the processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 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; or

4.1.6 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.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data" (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation)), at least one of the several conditions must be met. They are (in summary):

4.2.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes;

4.2.2 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;

4.2.3 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;

4.2.4 the data holder 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;

4.2.5 the processing relates to personal data which is clearly made public by the data subject;

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

4.2.7 the processing is necessary for substantial public interest reasons;

4.2.8 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 or pursuant to a contract with a health professional;

4.2.9 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; or

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

5. Specified, Explicit, and Legitimate Purposes

5.1 We collect and process the personal data of data subjects.

5.2 The specific purposes for which we collect, process and hold such personal data are set out below this Policy.

5.3 We aim to keep data subjects informed at all times of the purpose or purposes for which we use their personal data.

5.4 We will 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).

6. Accuracy of Data and Keeping Data Up-to-Date

6.1 We shall ensure that all personal data collected, processed and held by us is kept accurate and up-to-date. This includes the rectification of personal data at the request of a data subject.

6.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable and timely steps will be taken to amend or erase that data, as appropriate.

7. Data Retention

7.1 We shall 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.

7.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it in a timely manner.

8. Secure Processing

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.

9. Accountability and Record-Keeping

9.1 We will ensure that we always have a person in post responsible for the management and control of data ("Data Controller"). Data subjects will be notified of the identity of the Data Controller. In the event that certain obligations arise, we may appoint a Data Controller.

9.2 The Data Controller shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and with the GDPR and other applicable data protection legislation.

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

9.3.1 the name and details of the Company, our Data Controller, and any applicable third-party data processors;

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

9.3.3 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;

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

9.3.5 details of how long personal data will be retained by us; and

9.3.6 detailed descriptions of all technical and organisational measures taken by us to ensure the security of personal data.

10. Data Protection Impact Assessments

10.1 We will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data where there may be a high risk to the rights and freedoms of data subjects under the GDPR.

10.2 Data Protection Impact Assessments shall be overseen by the Data Controller and will address the following:

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

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

10.2.3 our objectives in collecting, holding and processing the personal data in question;

10.2.4 how personal data is to be used;

10.2.5 the parties who are to be consulted;

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

10.2.7 risks posed to data subjects;

10.2.8 risks posed both within and to the Company; and

10.2.9 proposed measures to minimise and handle identified risks.

11. Keeping Data Subjects Informed

11.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection.

11.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

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

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

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

11.3 The following information shall be provided:

11.3.1 details of the Company including, but not limited to, the identity of its Data Controller;

11.3.2 the purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

11.3.3 where applicable, the legitimate interests upon which we are justifying the collection and processing of the personal data;

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

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

11.3.6 where the personal data is to be transferred to a third party that is located outside of the European Economic Area, details of that transfer, including but not limited to the safeguards in place;

11.3.7 details of data retention;

11.3.8 details of the data subject's rights under the GDPR;

11.3.9 details of the data subject's right to withdraw their consent to our processing of their personal data;

11.3.10 details of the data subject's right to complain to the Information Commissioner's Office;

11.3.11 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; and

11.3.12 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.

12. Data Subject Access

12.1 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.

12.2 Data subjects wishing to make a SAR should do using a Subject Access Request Form, sending the form to our Data Controller.

12.3 Responses to SARs shall normally be made within one month of receipt, but 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 will be informed.

12.4 All SARs received will be handled by our Data Controller.

12.5 We do 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.

13. Rectification of Personal Data

13.1 Data subjects have the right to require us to rectify any of their personal data that is inaccurate or incomplete.

13.2 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.

13.3 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.

14. Erasure of Personal Data

14.1 Data subjects have the right to request that we erase the personal data it holds about them in the following circumstances:

14.1.1 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;

14.1.2 the data subject wishes to withdraw their consent to our holding and processing their personal data;

14.1.3 the data subject objects to our holding and processing their personal data (and there is no overriding legitimate interest to allow us to continue doing so);

14.1.4 the personal data has been processed unlawfully;

14.1.5 the personal data needs to be erased in order for us to comply with a particular legal obligation.

14.2 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.

14.3 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).

15. Restriction of Personal Data Processing

15.1 Data subjects may request that we cease processing the personal data it holds about them. If a data subject makes such a request, we will 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.

15.2 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).

16. Data Portability

16.1 Where data subjects have given their consent to us to process their personal data in by automated means, 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 GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

16.2 To facilitate the right of data portability, we will make available the applicable personal data to data subjects in a format that is compatible with formats used commonly in the commercial sector.

16.3 Where technically feasible, if requested by a data subject, personal data will be sent directly to the required data controller.

16.4 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.

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to our processing their personal data based on legitimate interests.

17.2 Where a data subject objects to our processing their personal data based on its legitimate interests, we will cease such processing immediately, unless it can be demonstrated 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.

17.3 Where a data subject objects to our processing their personal data for direct marketing purposes, we will cease such processing immediately.

17.4 Where a data subject objects to our processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". We need not comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18. Automated Decision-Making

18.1 We may use personal data in automated decision-making processes with respect to persons on whom we hold personal data.

18.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of

the decision from the Company.

18.3 This right does not apply in the following circumstances:

18.3.1 the decision is necessary for the entry into, or performance of, a contract between us and the data subject;

18.3.2 the decision is authorised by law; or

18.3.3 the data subject has given their explicit consent.

19. Profiling

19.1 We may use personal data for profiling purposes

19.2 When personal data is used for profiling purposes, the following shall apply:

19.2.1 clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

19.2.2 appropriate mathematical or statistical procedures shall be used;

19.2.3 technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

19.2.4 all personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

20. Personal Data

We hold personal data that is relevant to our customers and to other persons with whom we may do business. That personal data shall be collected, held, and processed in accordance with the data subjects' rights and our obligations under the GDPR and with this Policy. We may collect, hold and process the following personal data:

20.1 identification information relating to customers and/or persons working for customer;

20.2 name;

20.3 contact details;

20.4 age;

20.5 gender;

20.6 ethnicity;

20.7 nationality;

20.8 banking details;

20.9 credit rating information.

21. Data Security - Transferring Personal Data and Communications

We will ensure that the following measures are taken with respect to all communications and other transfers involving personal data (including, but not limited to, personal data relating to individuals):

21.1 all emails containing personal data must be encrypted;

21.2 all emails containing personal data must be marked "confidential";

21.3 personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

21.4 personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

21.5 personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

21.6 where personal data is to be sent by facsimile transmission, the recipient should be informed in advance of the transmission and should be required to wait by the fax machine to receive the data;

21.7 where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a confidential courier service with the recipient being required personally to sign for their receipt; and

21.8 all personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

22. Data Security – Storage

We will ensure that the following measures are taken with respect to the storage of personal data (including, but not limited to, personal data relating to individuals):

22.1 all electronic copies of personal data should be stored securely using passwords and data encryption;

22.2 all hardcopies of personal data, along with any electronic copies stored on physical, removable media, should be stored securely in a locked box, drawer, cabinet or similar;

22.3 all personal data stored electronically should be backed up daily with backups stored either offsite or onsite in a secure location. All backups should be encrypted;

22.4 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 the Data Controller, 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; and

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

23. Data Security - Disposal

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.

24. Data Security - Use of Personal Data

We will ensure that the following measures are taken with respect to the use of personal data:

24.1 no personal data may be shared informally, and if an employee, agent, sub-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 the Data Controller;

24.2 no personal data may be transferred to any employees, agents, contractors or other parties, whether such parties are working on our behalf or not, without the authorisation of the Data Controller;

24.3 personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

24.4 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; and

24.5 where personal data held us is used for marketing purposes, it shall be the responsibility of the director responsible for marketing to ensure that the appropriate consent is obtained and that no data subjects have opted out.

25. Data Security - IT Security

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

25.1 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;

25.2 under no circumstances should any passwords be written down or shared between any employees, agents, contractors or other parties working on our behalf, 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;

25.3 all software (including applications and operating systems) shall be kept up-to-date. Our IT staff will be responsible for installing any and all security-related updates in a timely and effective manner; and

25.4 no software may be installed on any Company-owned computer or device without the prior approval of the director responsible for IT management.

26. Employees

26.1 In the case of data subjects who are employees ("employee data subjects"), we hold the following personal data and such data will be collected, held and processed in accordance with this Policy):

26.1.1 name;

26.1.2 contact details;

26.1.3 equal opportunities monitoring information;

26.1.4 age;

26.1.5 gender;

26.1.6 ethnicity;

26.1.7 nationality;

26.1.8 religion;

26.1.9 sexual orientation;

26.1.10 marital status;

26.1.11 health records, including details of sick leave, medical conditions, disabilities, prescribed medication;

26.1.12 employment records, including interview notes, CVs, application forms, covering letters, and similar documents, assessments, performance reviews and similar documents;

26.1.13 details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits and expenses;

26.1.14 details of trade union membership (where applicable);

26.1.15 employee monitoring information;

26.1.16 records of disciplinary matters including reports and warnings, both formal and informal;

26.1.17 details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes.

26.2 We hold health records on employee data subjects which are used to assess the health, wellbeing and welfare of employees and to highlight any issues which may require further investigation. In particular, we place a high priority on maintaining health and safety in the workplace, on promoting equal opportunities and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the GDPR's definition of special category data. Any and all data relating to employee data subjects' health, therefore, will be collected, held and processed strictly in

accordance with the conditions for processing special category personal data. No special category personal data will be collected, held or processed without the relevant employee data subject's express consent.

26.3 Health records will be accessible and used only by the persons and departments (such as the human resources department) who need to know that information for legitimate corporate purposes and shall not be revealed to other employees, agents, contractors, or other parties working on our behalf, except in exceptional circumstances where the wellbeing of the employee data subject(s) to whom the data relates is at stake and all relevant conditions are met.

26.4 Health records will only be collected, held and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely and without unlawful or unfair impediments or discrimination.

26.5 Employee data subjects have the right to request that we do not keep health records about them. All such requests must be made in writing and addressed to the Data Controller.

26.6 In cases where employee data subjects are enrolled in benefit schemes which are provided by us, it may be necessary from time to time for third party organisations to collect personal data for relevant employee data subjects.

26.7 Prior to the collection of such data, employee data subjects will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.

26.8 We will not use any such personal data except insofar as is necessary in the administration of the relevant benefits schemes.

26.9 We will provide the following personal data concerning relevant employee data subjects to bona fide trade unions where those unions are recognised by us. In most cases, information about an individual's trade union membership falls within the GDPR's definition of special category data. Any and all data relating to employee data subjects' trade union membership, therefore, will be collected, held and processed strictly in accordance with the conditions for processing special category personal data. No special category personal data will be collected, held or processed without the relevant employee data subject's express consent. The following data will be collected and supplied:

26.9.1 name;

26.9.2 job description.

26.10 All employee data subjects have the right to request that we do not supply their personal data to trade unions and shall be informed of that right before any such transfer is made.

26.11 We may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

26.12 Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

26.13 Monitoring will only take place if we consider that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and our obligations under the GDPR.

26.14 We will ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using Company equipment or other facilities including,

but not limited to, Company email, the Company intranet, or a virtual private network ("VPN") service provided by us for employee use.

27. Organisational Measures

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

27.1 all employees, agents, contractors or other parties working on our behalf shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

27.2 only employees, agents, sub-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;

27.3 all employees, agents, contractors or other parties working on our behalf handling personal data will be appropriately trained to do so;

27.4 all employees, agents, contractors or other parties working on our behalf handling personal data will be appropriately supervised;

27.5 all employees, agents, contractors or other parties working on our behalf 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;

27.6 methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

27.7 all personal data held by us shall be reviewed periodically;

27.8 the performance of those employees, agents, contractors or other parties working on our behalf handling personal data shall be regularly evaluated and reviewed;

27.9 all employees, agents, contractors or other parties working on our behalf handling personal data will be bound contractually to do so in accordance with the principles of the GDPR and this Policy;

27.10 all agents, contractors or other parties working on our behalf 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 that apply to our employees who handle personal data; and

27.11 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.

28. Transferring Personal Data to a Country Outside the EEA

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

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

28.2.1 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;

28.2.2 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 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;

28.2.3 the transfer is made with the informed consent of the relevant data subject(s);

28.2.4 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);

28.2.5 the transfer is necessary for important public interest reasons;

28.2.6 the transfer is necessary for the conduct of legal claims;

28.2.7 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

28.2.8 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.

29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the Data Controller.

29.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Controller 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.

29.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Controller must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29.4 Data breach notifications shall include the following information:

29.4.1 the categories and approximate number of data subjects concerned;

29.4.2 the categories and approximate number of personal data records concerned;

29.4.3 the name and contact details of the Data Controller (or other contact point where more information can be obtained);

29.4.4 the likely consequences of the breach;

29.4.5 details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

30. Implementation of Policy

This Policy shall be deemed effective as of the date below. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after that date.

This Policy has been approved and authorised by:

Name: Robert Lumley

Position: Director

Date: 16th May 2018

Due for Review by: Managing Director

Signature: