New Red Planet: Data Protection Policy

1. Introduction

This Policy sets out how New Red Planet Limited (NRP), a company registered in England and Wales (under number 11924166), whose registered office is at Glasshouse, Suite 2F3, Alderley Park, Cheshire SK10 4ZE (the **Company**, **us**, **our** or **we**), handle personal data of our customers, suppliers, employees, workers and other third parties.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, directors, shareholders, website or mobile application users or any other data subject.

The procedures and principles set out in this Policy applies to all Company Personnel (**you** or **your**). You must read, understand and comply with this Policy when processing personal data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for NRP to comply with Data Protection Law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

This Policy is an internal document and cannot be shared with third parties, clients or regulators without the prior authorisation from the Data Protection Executive (as defined below).

Definitions

criminal convictions data	means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings;
Company Personnel	all employees, workers, contractors, consultants, directors, shareholders & others;
consent	means 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	means 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, the Company is the data controller of all personal data relating to Company Personnel & personal data used in our business for our commercial purposes;
data processor	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
Data Protection Executive (DPE)	appointed Executive who is accountable for data privacy;
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**), 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);
data subject	means a living, identified, or identifiable natural person about whom the Company holds personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data;
GDPR	has the meaning given to it in **Data Protection Law;**
personal data	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 identifies we possess or can reasonably access. Personal data including special categories of personal data and pseudonymised personal data but excludes anonymous personal data or data that has had the identity of an individual permanently removed. Personal data can be factual (i.e. a name, email address, location or dated or birth) or an opinion about that person's actions or behaviour;
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;
privacy policies or privacy notices (also known as fair processing notices)	separate notices setting out information that may be provided to data subjects when NRP 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 website privacy policy) or they may be stand-alone, one- time privacy statements covering processing related to a specific purpose;
processing	means 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 and **pseudonymised**	means 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; and
special category personal data	means 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.

2. Scope

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. NRP is exposed to potential fines of up to EUR 20 million or 4% of total worldwide turnover, whichever is the higher, depending on the breach, for failure to comply with the provisions of GDPR.

The Company's current Data Protection Executive is Phil Whelan. The DPE is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

Any questions relating to this Policy or to Data Protection Law should be referred to the DPE. In particular, the DPE 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; or

n) if you need help with any contracts or other areas in relation to sharing personal data with third parties.

3. The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject (**Lawfulness, Fairness and Transparency**);

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 (**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. 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 (**Accuracy**);

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 (**Storage Limitation**). 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 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 (**Security, Integrity and Confidentiality**);

g) not transferred to another country without appropriate safeguards being in place (**Transfer Limitations**); and

h) made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (**Data Subject's Rights and Requests**).

We are responsible for, and must be able to demonstrate, compliance with, the data protection principles listed above (**Accountability**).

4. The Rights of Data Subjects

The 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');

e) the right to restrict processing;

f) the right to data portability;

g) the right to object; and

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

5. 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 GDPR states that processing of personal data is restricted to the specified lawful purposes which are set out below:

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; or

f) the processing is necessary for the purposes of our legitimate interests, 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. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

6. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

a) 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.

b) 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.

c) 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.

d) 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.

e) If special category personal data or criminal convictions data is processed, the Company shall normally rely on a lawful basis other than explicit consent or consent if possible. If explicit consent or consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

f) 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 the Company can demonstrate its compliance with consent requirements.

7. Specified, Explicit, and Legitimate Purposes

The Company only collects, processes, and holds personal data for specified, explicit and legitimate purposes.

Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented, where necessary.

8. Adequate, Relevant, and Limited Data Processing

The Company 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) as under Part 8, above.

Company Personnel 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.

Company Personnel may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

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

The Company shall ensure that all personal data collected, processed, and held by it 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.

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 steps will be taken without delay to amend or erase that data, as appropriate.

10. Data Retention

The Company 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.

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

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

11. Secure Processing

The Company 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. Further details of the technical and organisational measures which shall be taken are provided in Parts 23 to 27of this Policy.

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. All Company Personnel are responsible for protecting the personal data that we hold and must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damaged to, personal data. You must exercise particular care in protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure.

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; and

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

You must follow all procedures and technologies that we put in place to maintain the security of all personal data from the point of collection to the point of destruction and you must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

12. Accountability and Record-Keeping

The DPE is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

The Company shall 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).

All Company Personnel 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.

The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

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

a) the name and details of the Company, its DPO (where applicable), and any applicable third- party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the Company collects, holds, and processes personal data;

c) the Company's 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;

d) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

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

f) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

g) details of personal data storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

13. Data Protection Impact Assessments and Privacy by Design

In accordance with the privacy by design principles, the Company 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.

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; and

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

Data Protection Impact Assessments shall be overseen by the DPE 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) the Company's 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 and to the Company; and

i) proposed measures to minimise and handle identified risks.

14. Keeping Data Subjects Informed

14.1 The Company shall provide the information set out in Part 14.2 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.

14.2 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;

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

c) where applicable, the legitimate interests upon which the Company is 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 27 of this Policy for further details);

g) details of applicable data retention periods;

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

i) details of the data subject's right to withdraw their consent to the Company's processing of 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 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; and

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.

15. Data Subject Access

Data subjects may make subject access requests (**SARs**) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why. You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authority).

You must immediately forward any SAR that you receive to the DPE and comply with the Company's SAR response process.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's DPE.

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.

All SARs received shall be handled by the Company's DPE.

The Company does not charge a fee for the handling of normal SARs. The Company reserves 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.

16. Rectification of Personal Data

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

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company 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.

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.

17. Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company 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 the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 19 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**.**

Unless the Company has 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.

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).

18. Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company 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.

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).

19. Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's 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.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

20. Direct Marketing

The Company is subject to certain rules and regulations when marketing its services.

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:

- The Company may 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 the Company.

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.

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.

21. Data Security - Transferring Personal Data and Communications

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

a) all emails containing personal data must be encrypted;

b) all emails containing personal data must be marked "confidential";

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

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

e) 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;

f) where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a reputable courier or registered first class post;

g) 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

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

a) all electronic copies of personal data should be stored securely using passwords and Advanced Encryption Standard (AES) with 256-bit keys data encryption;

b) 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;

c) 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;

d) no personal data should be transferred to any device personally belonging to any Company Personnel 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 GDPR (which may include demonstrating to the Company 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. For further information on the deletion and disposal of personal data, please refer to the Company's Data

Retention Policy.

24. Data Security - Use of Personal Data

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

a) no personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the DPE;

b) 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 the DPE;

c) 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;

d) 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;

e) where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the DPE 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.

25. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

a) 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.

b) 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;

c) all software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates, unless there are valid technical reasons not to do so; and

d) no software may be installed on any Company-owned computer or device without the prior approval of the IT Department.

26. Organisational Measures

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

a) all Company Personnel 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;

b) only Company Personnel 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;

c) 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;

d) all Company Personnel handling personal data will be appropriately trained to do so;

e) all Company Personnel handling personal data will be appropriately supervised;

f) all Company Personnel 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;

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

h) all personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

i) the performance of those Company Personnel handling personal data shall be regularly evaluated and reviewed;

j) all Company Personnel handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

k) 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;

l) where any agent, contractor or other party working on behalf of the Company 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.

27. Transferring Personal Data to a Country Outside the EEA

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

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

i) 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;

ii) 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;

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

iv) 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);

v) the transfer is necessary for important public interest reasons;

vi) the transfer is necessary for the conduct of legal claims;

vii) 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

viii) 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.

28. Data Breach Notification

All personal data breaches must be reported immediately to the Company's DPE.

If any Company Personnel 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.

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), the DPE 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.

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 DPE must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

a) the categories and approximate number of data subjects concerned;

b) the categories and approximate number of personal data records concerned;

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

d) the likely consequences of the breach; and

e) 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.

Date of Review: January 2028