Data Protection – Data Security Policy

General

This policy forms part of the Company's suite of data protection policies. It is drafted so as to comply with the GDPR (General Data Protection Regulation) which comes into force in England on the 25th of May 2018 and which replaces the Data Protection Act 1998.

This policy sets out the Company's position on data security including (but not limited to) security of personal data as defined by Data Protection legislation. For the purposes of this policy, "data" includes "personal data" as defined in the Headline Data protection policy but also all information belonging to the Company or in the possession of the Company which is of a sensitive or confidential nature.

This policy may be made public to data subjects, including employees and others engaged in providing services to the Company.

This policy has contractual effect within the organistion and all employees and others engaged in providing services to the Company are expected to abide by it.

This policy should be read in conjunction with the Company's headline Data Protection Policy and the Data Protection Policy – Breach Reporting which sets out the specific procedures that must be followed in the event that a breach of the Company's data protection policies has occurred.

Legal Framework

Data protection legislation requires that organisations process personal data in a manner that ensures its security. This includes ensuring protection against unauthorised or unlawful processing and against loss, destruction or damage.

Organisations must put in place policies to ensure that only authorised people can access, alter, disclose or destroy personal data, that everyone acts within the scope of their authority and that so far as possible, breaches are drawn to the attention of the organisation and steps are taken to minimise the effect of any breaches and to recover any lost data so as to prevent damage or destress to affected data subjects.

The more sensitive the data an organisation holds, the greater measures that the organisation should take to protect it.

Outside the sphere of data protection, organisations are entitled to protect confidential information and trade secrets and may also be bound to protect formation provided by third parties which is of a sensitive or personal nature.

Data Security Measures – Employees and Contractors

All employees and those engaged in providing services to the Company are expected to abide by the following data security measures:-

a) Data may be transmitted only over secure networks. Transmission over unsecured networks is not permitted in any circumstances. The Company's computer network is a secure network but employees should not send data from their own e-mail accounts or from other networks (including mobile phone networks) without seeking the advance permission of their manager and (where the information to be sent includes personal data) the data protection officer.

b) Incoming and outgoing e-mails will be stored on the Company's e-mail system. E-mails will be deleted from time to time. Any data contained in the body of an e-mail (whether sent or

received) which needs to be kept for any period of time should be stored securely. Where that data is personal data, it should only be copied and stored where it is necessary to do so for one or more purposes outlined in the Company's privacy notices.

c) Where data is to be sent by facsimile transmission, wherever possible the recipient should be informed in advance of the transmission.

d) Where data is to be transferred in hard copy form it should be passed directly to the recipient or sent using the recipient's name and marked "private & confidential – for addressee only".

e) No data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to and/or are not entitled to access in the normal course of performing their duties, such access should be formally requested from the data protection officer.

f) All hard copies of data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.

g) Desks should be left clear at the end of each working day and hard copies of data should not be left on desks unless the room in which the data is located can be locked.

h) No data may be transferred other than in the normal course of business to any person, whether such parties are working on behalf of the Company or not, without the advance authorisation of the data protection officer.

i) 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;

j) If 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.

k) All computer users should log out of the computer system when they finish work for the day and switch the system off. Do not simply leave the system on standby.

l) Any unwanted copies of data (i.e. printouts or electronic duplicates) that are no longer needed should be disposed of securely. Hard copies should be shredded and electronic copies should be deleted permanently.

m) No data should be transferred to any device personally belonging to an employee save with the express permission of your manager or the data protection officer.

n) 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 this policy, with Data Protection legislation and with confidentiality more widely, which may include demonstrating to the Company that all suitable technical and organisational measures have been taken.

o) All data stored electronically should be backed up and the Company shall put in place such measures as are necessary to ensure the regular backing up of data. Wherever possible, all backups will be encrypted.

p) All passwords used to protect 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.

q) 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.

r) All data held by the Company shall be regularly reviewed for accuracy and completeness. Where the Company has regular contact with data subjects, any data held about those data subjects should be confirmed regularly. If any data is found to be out of date or otherwise inaccurate, it should be updated and/or corrected immediately where possible. If any data is no longer required by the Company, it should be securely deleted and disposed of.

s) Where data held by the Company is used for marketing purposes, only authorised employees may carry out marketing activities. No other employee is authorised to carry out such activities.

t) Any request for references must be handled by the HR department and/or a director of the company. No employee is authorised to write a reference for a fellow employee or ex-employee which in any way mentions the Company or makes any comment about that employee or ex-employee's abilities to do their job or their suitability for another post. Personal references may be given provided they are first approved by the HR department or a director of the Company.

Data Security Measure – Company Obligations

The Company shall ensure that:-

a) All employees, agents, contractors, or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under data protection legislation and under the Company's suite of data protection policies , and, where necessary, shall be provided with a copy of the Company's suite of data protection policies.

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

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

d) All employees, agents, contractors, or other parties working on behalf of the Company handling data will be appropriately supervised.

e) Methods of collecting, holding and processing data shall be regularly evaluated and reviewed.

f) All employees, agents, contractors, or other parties working on behalf of the Company handling data will be bound to do so in accordance with the principles of data protection legislation and the Company's data protection policies.

g) All agents, contractors, or other parties working on behalf of the Company handling data must ensure that any and all of their employees who are involved in the processing of data are held to the same conditions as those which apply to employees of the Company.

h) Where any agent, contractor or other party working on behalf of the Company handling data fails in their obligations regarding personal data or confidential information, wherever practicable 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.

Data Storage and Data Sharing

[To be used if data will remain in UK] The Company will only store or transfer personal data in the UK.

This means that it will be fully protected under the GDPR.

OR

[To be used if data will be stored in UK or in European Economic Area] The Company will only store or transfer personal data within the European Economic Area (the "EEA"). The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein. This means that personal data will be fully protected under the GDPR or to equivalent standards by law.

OR

[To be used if data may be sent outside the UK or the European Economic Area] The Company may store or transfer personal data in countries that are not part of the European Economic Area (the "EEA" consists of all EU member states, plus Norway, Iceland, and Liechtenstein). These are known as "third countries" and may not have data protection laws that are as strong as those in the UK and/or the EEA. Where personal data is stored or transferred outside the EEA, the Company will take appropriate steps in order to ensure that personal data is treated just as safely and securely as it would be within the UK and under the GDPR.

Data Sharing

[To be used if Company is part of a group of companies] The Company may share personal data within the group of companies of which the Company is a part. All companies within the group must follow the same rules with respect to data usage. Where data is shared with companies outside the EEA, certain rules apply. These are known as "binding corporate rules". More information on binding corporate rules is available from the ICO website (https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/).

[AND/OR]

[To be used if data may be shared outside the UK or the European Economic Area other than with group companies] The Company may share personal data with external third parties that are based outside the EEA. If so, the Company will only transfer personal data to countries that the European Commission has deemed to provide an adequate level of data protection. More information is available from the European Commission.**]**

[AND/OR]

The Company use specific contracts with external third parties that are approved by the European Commission for the transfer of data to third party countries. These contracts ensure the same levels of data protection that would apply under the GDPR. More information is available from the European Commission.**]**

[AND/OR]

If the Company transfers personal data to a third party based in the US, the data may be protected if the transferee is part of the EU-US Privacy Shield. This requires that third party to provide data protection to standards similar levels of data protection to those in Europe. More information is available from the European Commission.**]**

[IN EVERY CASE]

Please contact (insert details of data protection officer, company name and e-mail address) for further information about the particular data protection mechanisms used by the Company when transferring personal data to another country.