DATA PROTECTION POLICY

1. DATA PROTECTION POLICY

1.1 This policy sets out how personal information is handled within the Company ("We", "Us"). During the course of our activities we will collect, store and process personal information about our stakeholders, and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, interns, suppliers, customers, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and other regulations. The Act imposes restrictions on how we may use that information. We have updated this policy to comply with the UK General Data Protection Regulation (UK-GDPR) that came into force upon the UK's departure from the European Union in January 2021. We reserve the right to change or amend this policy as necessary.

2. STATUS OF THE POLICY

2.1 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce, browsers, prospective customers, product users, customers, supply chain participants and suppliers ("Stakeholder", "Data Subjects"). Its purpose is also to ensure that the company understand and comply with the rules governing the collection, use and deletion of personal information to which we have access to in the course of our work.

2.2 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our Stakeholders, and how (and when) we delete that information once it is no longer required.

2.3 The Company's Data Protection Manager/Officer ("DPO/M"), is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If any Data Subject has any questions or comments about the content of this policy the DPO/M.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** (sometimes known as personal information) means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

3.5 **Criminal records information** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3.6 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. Our Risk Compliance and Operations (RCO) department is collectively the data controller of all personal data used in our business.

3.7 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.8 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.9 **Data Protection Officer (DPO)**. DPOs are responsible for educating the company and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data. Many companies are not required to have an official DPO and it is undecided as to whether the Company shall employ an official DPO and so the term DPO/M is used to assign someone who carries DPO duties but is not officially a DPO.

3.10 **Processing information** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it.

3.11 **Pseudonymised** means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

3.12 **Sensitive personal data** (sometimes known as “special categories of data”) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership or non-membership, physical or mental health or condition or sexual life or sexual orientation or genetics information or biometric information (where used to identify an individual) or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

4.1 The Company will comply with the following data protection principles when processing personal information:

(a) we will process personal information lawfully, fairly and in a transparent manner;

(b) we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

(c) we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

(d) we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

(e) we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

(f) we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. BASIS FOR PROCESSING PERSONAL INFORMATION

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

(a) review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(i) that the data subject has consented to the processing;

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

(iii) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(iv) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 11 below.

(b) except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);

(i) document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

(ii) include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

(iii) where sensitive personal information is processed, also identify a lawful special condition for processing that information (see clause 6) and document it; and

(iv) where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

(a) conduct a legitimate interests assessment (LIA) as set out in Appendix 2 and keep a record of it, to ensure that we can justify our decision;

(b) if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

(c) keep the LIA under review, and repeat it if circumstances change; and

(d) include information about our legitimate interests in our relevant privacy notice(s).

6. SENSITIVE PERSONAL INFORMATION

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'. The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

(a) we have a lawful basis for doing so as set out in paragraph 5.1(a) above, eg it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

(b) one of the special conditions for processing sensitive personal information applies, eg:

(i) the data subject has given has given explicit consent;

(ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(iv) processing relates to personal data which are manifestly made public by the data subject;

(v) the processing is necessary for the establishment, exercise or defence of legal claims; or

(vi) the processing is necessary for reasons of substantial public interest.

6.2 Before processing any sensitive personal information, staff must notify the DPO/M of the proposed processing, in order that the DPO/M may assess whether the processing complies with the criteria noted above.

6.3 Sensitive personal information will not be processed until:

(a) the assessment referred to in paragraph 6.1 has taken place; and

(b) the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.4 The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6.5 The Company's Data Protection Privacy Notice sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

6.6 In relation to sensitive personal information, the Company will comply with the procedures set out in paragraphs 9.1 and 9.2 below to make sure that it complies with the data protection principles set out in paragraph 6.3 above.

6.7 **During the recruitment process**: the HR department, with guidance from the DPO/M will ensure that (except where the law permits otherwise):

(a) during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;

(b) if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

(c) any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

(d) we will only ask health questions once an offer of employment has been made.

6.8 **During employment**: the HR department, with guidance from the DPO/M will process health information for the purposes of administering sick pay, keeping sickness

absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

7. CRIMINAL RECORDS INFORMATION

7.1 Criminal records information will be processed during the recruitment process before making a final decision to recruit. This information will be received from the candidate and from the Disclosure and Barring Service ("DBS") and we will request CRC (Criminal Record Certificates) for certain positions of trust. This information will be used to make an informed recruitment decision. If the candidate is successful we will retain the information in a secure cabinet for 6 years post-employment. If the candidate is unsuccessful then we will retain the information for 6 months in a secure cabinet and the data will then be destroyed unless required for legal requirements.

8. DATA PROTECTION IMPACT ASSESSMENTS

31.30 Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA as referenced in Appendix 1 to assess:

(a) whether the processing is necessary and proportionate in relation to its purpose;

(b) the risks to individuals; and

(c) what measures can be put in place to address those risks and protect personal information.

8.31 Before any new form of technology is introduced, the manager responsible should therefore contact the DPO/M in order that a DPIA can be carried out.

9. DOCUMENTATION AND RECORDS

9.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

(a) the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO/M);

(b) the purposes of the processing;

(c) a description of the categories of individuals and categories of personal data;

(d) categories of recipients of personal data;

(e) where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

(f) where possible, retention schedules; and

(g) where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

(a) information required for privacy notices;

(b) records of consent;

(c) controller-processor contracts;

(d) the location of personal information;

(e) DPIAs; and

(f) records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

(a) the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

(b) the lawful basis for our processing; and

(c) whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include talking to staff across the Company to get a more complete picture of our processing activities and reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9.5 We document our processing activities in electronic form so we can add, remove and amend information easily.

10. PRIVACY NOTICE

10.1 The Company will issue privacy notices from time to time, informing stakeholders about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11. INDIVIDUAL RIGHTS

11.1 Data Subjects have the following rights in relation to their personal information:

(a) to be informed about how, why and on what basis that information is processed—see the Company's Data Protection privacy notice.;

(b) to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Company's subject access form and process in Appendix 3;

(c) to have data corrected if it is inaccurate or incomplete;

(d) to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

(e) to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the employer no longer needs the personal information but they require the data to establish, exercise or defend a legal claim; and

(f) to restrict the processing of personal information temporarily where they do not think it is accurate (and the employer is verifying whether it is accurate), or where they have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override they interests).

11.2 If Data Subjects wish to exercise any of the rights in paragraphs 11.1a to 11.1f they must contact the DPO/M .

12. INDIVIDUAL OBLIGATIONS

12.1 Individuals are responsible for helping the Company keep their personal information up to date. Data Subjects should let the Company know if the information that has been previously provided to the Company changes, for example if a stakeholder moves house or bank account details change.

12.2 Stakeholders may have access to the personal information of other stakeholders (particularly Company employees). If so, the Company expects its employees to help meet its data protection obligations to those individuals. For example, they should should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If staff have access to personal information, they must:

(a) only access the personal information that they have authority to access, and only for authorised purposes;

(b) only allow other Company staff to access personal information if they have appropriate authorisation;

(c) only allow individuals who are not Company staff to access personal information if they have specific authority to do so from their supervisor.

(d) keep personal information secure, this includes by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's Information Security policy.

(e) Company security procedures include:

(i) **Access controls.** Any staff seen in entry-controlled areas should be reported or unauthorised drives, applications or devices.

(ii) **Methods of disposal.** Paper documents should be shredded. Removable media is banned but if used, they must be wiped afterwards.

(iii) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

(f) not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

(g) not store personal information on local drives or on personal devices that are used for work purposes.

12.4 Staff should contact the DPO/M if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

(a) processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.1(b) being met;

(b) any data breach as set out in clause 15 below;

(c) access to personal information without the proper authorisation;

(d) personal information not kept or deleted securely;

(e) removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

(f) any other breach of this policy or of any of the data protection principles.

13. INFORMATION SECURITY

13.1 The Company will use appropriate technical and organisational measures in accordance with the Company's information security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

(a) making sure that, where possible, personal information is pseudonymised or encrypted;

(b) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements will be implemented in contracts with those

organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

(a) the organisation may act only on the written instructions of the Company;

(b) those processing the data are subject to a duty of confidence;

(c) appropriate measures are taken to ensure the security of processing;

(d) sub-contractors are only engaged with the prior consent of the Company and under a written contract;

(e) the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;

(f) the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

(g) the organisation will delete or return all personal information to the Company as requested at the end of the contract; and

(h) the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DPO/M.

14. STORAGE AND RETENTION OF PERSONAL INFORMATION

14.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's Information Security Policy.

14.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Company's Retention and Erasure policy which set out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the DPO/M.

14.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15. DATA BREACHES

15.1 A data breach may take many different forms, for example:

(a) loss or theft of data or equipment on which personal information is stored;

(b) unauthorised access to or use of personal information either by a member of staff or third party;

(c) loss of data resulting from an equipment or systems (including hardware and software) failure;

(d) human error, such as accidental deletion or alteration of data;

(e) unforeseen circumstances, such as a fire or flood;

(f) deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

(g) 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 The Company will:

(a) make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

(b) notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16. INTERNATIONAL TRANSFERS

16.1 The Company will only transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to another country on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of

binding corporate rules OR standard data protection clauses OR of compliance with an approved code of conduct.

17. TRAINING

17.1 The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18. UK-GDPR COMPLIANCE FAILURES

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

(a) puts at risk the individuals whose personal information is being processed; and

(b) carries the risk of significant civil and criminal sanctions for the individual and the Company; and

(c) may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

19. APPENDICES (INTENTIONALLY REDACTED)

APPENDIX 1: DATA PROCESSING IMPACT ASSESSMENT

APPENDIX 2: LEGITIMATE INTEREST IMPACT ASSESSMENT

APPENDIX 3: DATA SUBJECT ACCESS REQUEST FORM

APPENDIX 4: BREACH NOTIFICATION FORM (INFORMATION SECURITY INCIDENT FORM)

APPENDIX 5: BREACH INVESTIGATION PROCESS