DATA PROTECTION POLICY (PERSONAL DATA PRIVACY STANDARD)

TABLE OF CONTENTS

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their Personal Data is handled. During

the course of our activities we will collect, store and process Personal Data about our staff, suppliers, customers and any others we communicate with, and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of Personal Data that we may be required to handle include details of current, past and prospective employees, other staff, 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 UK General Data Protection Regulation (GDPR) and other UK data protection law. These laws impose restrictions on how we may use that Personal Data.

1.3 We have a commitment to ensuring that Personal Data is processed in line with UK GDPR and relevant UK law and that all our staff conduct themselves in line with this and other related policies. Where third parties process Personal Data on our behalf, we will ensure that the third party takes the necessary measures to maintain our commitment to protecting Personal Data.

1.4 This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of Personal Data.

1.5 If you consider that this policy has not been followed in respect of Personal Data about yourself or others, you should raise the matter with the Privacy Officer, your manager or a Director.

1.6 This Data Protection Policy, also known as our Personal Data Privacy Standard, does not form part of any employee's contract of employment and it may be amended at any time. We may also vary elements, such as any time limits, as appropriate in any case. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. WHO IS COVERED BY THIS POLICY?

2.1 This policy applies to all employees, directors and other officers, workers and agency workers, volunteers and interns.

2.2 We also require in any contracts with third parties who may have access to any Personal Data, such as consultants, contractors or suppliers, that they comply with this policy. We will ensure they are given access to a copy.

2.3 All individuals covered in sections 2.1 and 2.2 are referred to as 'staff' in this policy.

3. WHO IS RESPONSIBLE FOR THIS POLICY?

3.1 Our Privacy Officer is responsible for ensuring compliance with UK GDPR and with this policy. your manager can advise you who our Privacy Officer is. If we have cause to appoint a Data Protection Officer (an official appointment) or use a different title for our Privacy Officer, we will let you know, and any reference to Privacy Officer shall include reference to a new title or a Data Protection Officer.

3.2 While we ask all managers to work with the Privacy Officer to make sure this policy is complied with, its successful operation also depends on you. Please take the time to read and understand it, and to go back to the Privacy Officer or your manager with any questions you may have. References to Directors in this policy mean the most senior people within our organisation.

4. DEFINITION OF DATA PROTECTION TERMS

4.1 **Personal Data** in this policy is personal data about an individual who can be directly or indirectly identified from that information. 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).

4.2 **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. Individuals should be allowed to exercise their rights in relation to their Personal Data, and Personal Data about them should be made available to individuals who request it.

4.3 **Data Controllers** are the people who or organisations that 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 relevant laws. We are the Data Controller of all Personal Data used in our business.

4.4 **Data Users** include staff whose work involves using Personal Data. Data Users have a duty to protect the Personal Data they handle by following our policies relating to the protection and security of Personal Data at all times. All staff have a responsibility, when using Personal Data, to comply with any security safeguards and procedures we put in place.

4.5 **Data Processors** include any people who or organisations that process Personal Data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition, but it could include third-party suppliers which handle Personal Data on our behalf.

4.6 **Processing** is almost any activity that involves use of Personal Data. It includes obtaining, recording or holding Personal Data, or carrying out any operation or set of operations on Personal Data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

4.7 **Special Categories of Data** are sensitive categories of Personal Data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life, or sexual orientation. It also includes genetic and biometric Data (where used for ID purposes). Special Categories of Data can only be processed under strict conditions, and may require the explicit consent of the person concerned.

4.8 **Criminal Offence Data** is Personal Data that relates to an individual's criminal convictions and offences. It can only be processed under strict conditions, and may require the explicit consent of the person concerned.

4.9 **Data Breach** is any act or omission which compromises the security, confidentiality, integrity or availability of Personal Data, or the safeguards that we or a third party put in place to protect the Personal Data, including losing the Personal Data or disclosing it to unauthorised people.

5. DATA PROTECTION PRINCIPLES

5.1 Anyone processing Personal Data must comply with the eight enforceable principles of good practice. These provide that Personal Data must be:

a) processed fairly, lawfully and in a transparent manner (**Fairness, Lawfulness and Transparency**),

b) processed for specified, explicit and legitimate purposes and in an appropriate way (**Purpose Limitation**),

c) adequate, relevant and limited to what is necessary for the stated purpose (**Data Minimisation**),

d) kept accurate and up to date (**Accuracy**),

e) not kept longer than necessary for the stated purpose (**Storage Limitation**),

f) processed in a manner that ensures appropriate security of Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures (**Security, Integrity and Confidentiality**),

g) not transferred to another country without appropriate safeguards being in place.(**Transfer Limitation**), and

h) processed in line with Data Subjects' rights (**Data Subject's Rights and Requests**).

5.2 We are responsible for and need to demonstrate compliance with the data protection principles listed above (**Accountability**).

6. FAIRNESS AND LAWFULNESS

6.1 The purpose of UK GDPR and UK data protection laws is not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.

6.2 UK GDPR allows processing of Personal Data for specific purposes, which are where it is needed:

a) for the performance of a contract, such as an employment contract,

b) to comply with a legal obligation,

c) in order to pursue our legitimate interests (or those of a third party) and where the interests and fundamental rights of the Data Subject do not override those interests,

d) to protect the Data Subject's vital interests,

e) in the public interest, or

f) in situations where the Data Subject has given explicit consent.

6.3 We, as Data Controller, will only process Personal Data on the basis of one or more of the lawful bases set out in 6.2 above. Where consent is required, it is only effective if freely given, specific, informed and unambiguous. The Data Subject must be able to withdraw consent easily at any time, and any withdrawal will be promptly honoured.

6.4 Special Categories of Data and Criminal Convictions Data will only be processed with explicit consent of the Data Subject, unless the Data Controller can rely on one or more of the other lawful bases set out in 6.2 above, and any additional legal bases for processing specific to these types of data, details of which have been set out in an appropriate Privacy Notice issued to the Data Subject.

7. TRANSPARENCY

7.1 We will provide all required, detailed and specific information to Data Subjects about the use of their Personal Data through appropriate Privacy Notices, which will be concise, transparent, intelligible, easily accessible and in clear and plain language.

7.2 The Data Subject will be told:

a) who the Data Controller is (we, as your employer, are the Data Controller for HR Data),

b) who the Data Controller's representative is (in this case the Privacy Officer),

c) what Personal Data we collect from them,

d) the purpose for which the Personal Data is to be processed by us,

e) the legal basis for doing so,

f) the identities of anyone to whom the Personal Data may be disclosed or transferred,

g) how we protect their Personal Data, and

h) how long we will keep their Personal Data.

8. PURPOSE LIMITATION

8.1 Personal Data may only be processed for the specific purposes notified to the Data Subject via the Privacy Notice. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Personal Data is processed, the Data Subject must be informed of the new purpose via a new or amended Privacy Notice before any processing occurs.

9. DATA MINIMISATION

9.1 Personal Data should only be collected to the extent that it is required for the specific purposes notified to the Data Subject in the Privacy Notice. Any Personal Data that is not necessary for those purposes should not be collected in the first place.

10. ACCURACY

10.1 Personal Data must be accurate, complete and kept up to date. Information that is incorrect is not accurate, and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Personal Data should be amended or destroyed.

11. STORAGE LIMITATION

11.1 Personal Data should not be kept longer than is necessary to carry out the specified purposes. This means that Personal Data should be destroyed or erased from our systems when it is no longer required, and in accordance with our Data Retention Policy.

12. SECURITY, INTEGRITY AND CONFIDENTIALITY

12.1 We will ensure that appropriate technical and organisational security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

12.2 We will put in place procedural and technological safeguards appropriate to our size, scope and business, our available resources and the amount of Personal Data we hold, to maintain the security of all Personal Data, from the point of

collection to the point of destruction.

12.3 We will consider and use, where appropriate, the safeguards of encryption, anonymisation and pseudonymisation (replacing identifying information with artificial information so that the Data Subject cannot be identified without the use of additional information which is kept separately and secure).

12.4 We will regularly evaluate and test the effectiveness of these safeguards. Staff have a responsibility to comply with any safeguards we put in place.

12.5 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) confidentiality means only people who are authorised to use the Personal Data can access it,

b) integrity means Personal Data should be accurate and suitable for the purpose for which it is processed, and

c) availability means authorised users should be able to access Personal Data if they need it for authorised purposes.

12.6 Failure to follow rules on data security may be dealt with under our Disciplinary Procedure.

13. TRANSFER LIMITATION

13.1 The UK GDPR restricts Personal Data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

13.2 We may only transfer Personal Data outside the UK if one of the following conditions applies:

a) the UK has officially confirmed that the country to which the Personal Data is being transferred has an adequate level of protection for the Data Subject's rights and freedoms,

b) appropriate safeguards are in place, such as binding corporate rules or standard contractual clauses approved for use in the UK, or an approved code of conduct or a certification mechanism exists,

c) the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks, or

d) the transfer is necessary for one of the other reasons set out in the UK GDPR, such as the performance of a contract between us and the Data Subject; reasons of public interest; to establish, exercise or defend legal claims; to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent; or, in some limited cases, for our legitimate interest.

14. DATA SUBJECT'S RIGHTS AND REQUESTS

14.1 Personal Data must be processed in line with Data Subjects' rights. Data Subjects have the following rights, which apply in certain circumstances.

a) The right to be informed about processing of Personal Data.

b) The right of access to their own Personal Data.

c) The right for any inaccuracies to be corrected (rectification).

d) The right to have information deleted (erasure).

e) The right to restrict the processing of Personal Data.

f) The right to portability.

g) The right to object to the processing of their Personal Data.

h) The right to regulate any automated decision-making and profiling of Personal Data.

i) The right to withdraw consent when the only legal basis for processing Personal Data is consent.

j) The right to be notified of a Data Breach that is likely to result in high risk to their rights and freedoms.

k) The right to make a complaint to the Information Commissioner's Office or other supervisory authority.

14.2 If you receive a request from a Data Subject for details of Personal Data that we hold about them (Data Subject Access Request) you should forward it to [your manager] immediately.

15. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING (ADM)

15.1 Specific further rules to protect Data Subjects apply to any Automated Processing (including Profiling) and ADM related to their Personal Data.

15.2 Where you are involved in any data-processing activity by us that involves profiling or ADM, you must comply with any separate guidelines we issue on profiling or ADM.

16. DIRECT MARKETING

16.1 We are also subject to further rules and privacy laws about the processing of Personal Data when marketing to our customers.

16.2 You must comply with any separate guidelines we issue on direct marketing to customers.

17. BREACH NOTIFICATION

17.1 Where a Data Breach is likely to result in a risk to the rights and freedoms of the individual(s) concerned, we will report it to the Information Commissioner's Office within 72 hours of us becoming aware of it, and it may be reported in more than one instalment.

17.2 Individuals will be informed directly if the breach is likely to result in a high risk to their rights and freedoms.

17.3 If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

17.4 If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself, but contact the Privacy Officer, your manager or a Director immediately. You should preserve all evidence relating to the potential Data Breach.

17.5 For further information on our Data Breach procedure, please refer to our Personal Data Breach Policy.

18. TRAINING

18.1 New employees must read and understand this policy as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential Data Breach. All employees are trained to protect individuals' Personal Data to which they have access, to ensure data security and to understand the consequences to themselves and us of any potential breaches of the provisions of this policy.

18.2 Staff who are not employees will be required to familiarise themselves with this policy and comply with its obligations in relation to the obtaining, handling, processing, storage, transportation and destruction of Personal Data on our behalf.

19. RECORDS

19.1 We will keep full and accurate records of all our Personal Data processing activities.

20. MONITORING AND REVIEW OF THE POLICY

20.1 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.