Data Protection Policy

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

1.1.1 Introduction

1.2 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number specific lawful purposes.

1.3 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.4 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 workforce, and how (and when) we delete that information once it is no longer required.

1.5 The Company's data protection officer, Danielle Coletti, 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 you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer.

1.5.1 Scope

1.6 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

1.7 Staff should refer to the Company's data protection privacy notice and, where appropriate, to its other relevant policies including in relation to internet, email and communications, monitoring, social media, information security, data

retention and criminal record information, which contain further information regarding the protection of personal information in those contexts.

1.8 We will review and update this policy at least annually in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

1.8.1 Definitions

criminal records information	1**means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;**
data breach	2**means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;**
data subject	3**means the individual to whom the personal information relates;**
personal information	4**(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;**
processing information	5**means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;**
pseudonymised	6**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;**
sensitive personal information	7**(also known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.**

1.8.2 Data protection principles

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

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

1.9.2 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;

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

1.9.4 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;

1.9.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

1.9.6 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.

1.9.7 Basis for processing personal information

1.10 We will only process personal data where we have a legal justification for doing so, which will be set out in the Company's data protection privacy notice.

1.10.1 Sensitive personal information

1.11 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

1.12 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

1.12.1 we have a lawful basis for doing so as set out above, e.g. 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

1.12.2 one of the special conditions for processing sensitive personal information applies.

1.13 The Company's data protection privacy notice will set out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

1.13.1 Criminal records information

1.14 Where we are required by law to carry out criminal record checks then we will do so and the information received will be used to make the appropriate recruitment / employment decision and then destroyed. We will not retain criminal records information for any more than 6 months.

1.14.1 Privacy notice

1.15 The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

1.16 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.

1.16.1 Individual rights

1.17 You (in common with other data subjects) have the following rights in relation to your personal information:

1.17.1 to be informed about how, why and on what basis that information is processed—see the relevant data protection privacy notices;

1.17.2 to obtain confirmation that your 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 request policy;

1.17.3 to have data corrected if it is inaccurate or incomplete;

1.17.4 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');

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

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

1.18 If you wish to exercise any of these rights please contact the data protection officer.

1.18.1 Individual obligations

1.19 Individuals are responsible for helping the Company keep their personal information up to date. You should let the Company know if the information you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid.

1.20 You may have access to the personal information of other members of staff, suppliers and customers/clients of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.

1.21 If you have access to personal information, you must:

1.21.1 only access the personal information that you have authority to access, and only for authorised purposes;

1.21.2 only allow other Company staff to access personal information if they have appropriate authorisation;

1.21.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the data protection officer;

1.21.4 keep personal information secure (e.g. 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);

1.21.5 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

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

1.22 You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

1.22.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the lawful conditions being met;

1.22.2 any data breach as set out below;

1.22.3 access to personal information without the proper authorisation;

1.22.4 personal information not kept or deleted securely;

1.22.5 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;

1.22.6 any other breach of this policy or of any of the data protection principles set out in paragraph 1.9 above.

1.22.7 Information security

1.23 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

1.23.1 Storage and retention of personal information

1.24 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's obligations.

1.25 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.

1.26 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.

1.26.1 Data breaches

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

1.27.1 loss or theft of data or equipment on which personal information is stored;

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

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

1.27.4 human error, such as accidental deletion or alteration of data;

1.27.5 unforeseen circumstances, such as a fire or flood;

1.27.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

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

1.27.8 Training

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.

1.27.9 Consequences of failing to comply

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

1.28.1 puts at risk the individuals whose personal information is being processed; and

1.28.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

1.28.3 may, in some circumstances, amount to a criminal offence by the individual.

1.29 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.

1.30 If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

I have read and understood this policy and agree to abide by its terms.

Signed .....

Name .....

Date .....