DATA PROTECTION (EMPLOYEES & WORKERS) POLICY

Introduction

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 of specific lawful purposes, as set out in the Company's data protection privacy notices relating to recruitment and employment.

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 employees 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.

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.

Mark Woodcock, Data Protection Officer (DPO) is responsible for data protection compliance within the Company. Any questions or comments about the content of this policy should be directed to Mark by email (mwoodcock@jobmatcha.com).

Scope

This policy applies to the personal information of job applicants and current and former employees as well as temporary and agency workers, interns, volunteers and apprentices (referred to as "employees" in this policy).

Employees should refer to the Company's data protection privacy notice (employees and workers) and, where appropriate, to its other relevant policies including in relation to internet, email and communications, monitoring, social media, information security which contain further information regarding the protection of personal information in those contexts.

Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
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;
sensitive personal information	(sometimes known as 'special categories of personal data', 'special category 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.

Data protection principles

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

- we will process personal information lawfully, fairly and in a transparent manner;
- 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;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- 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
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for processing personal information

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

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.
    - that the data subject has consented to the processing;
    - 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;
    - that the processing is necessary for compliance with a legal obligation to which the Company is subject;
    - for the performance of a task carried out in the public interest;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - 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.

- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- insofar as is required by law, document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- insofar as is required by law, include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s); and
- where sensitive personal information is processed, also identify a lawful special condition for processing that information and, insofar as is required by law, document it.

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

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant privacy notice(s).

Sensitive personal information

Sensitive personal information is sometimes referred to as 'special categories of personal data' 'special category 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:

- we have a lawful basis for doing so, 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
- one of the special conditions for processing sensitive personal information applies, e.g.
    - the data subject has given explicit consent;
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;
    - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
    - processing relates to personal data which are manifestly made public by the data subject;

- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

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

Sensitive personal information will not be processed until:

- the assessment by the DPO has taken place; and
- 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.

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

The Company's data protection privacy notice (employees and workers) sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

In relation to sensitive personal information, the Company will comply with the procedures set out below in respect of the recruitment process and during employment to make sure that it complies with the data protection principles set out under **Data protection principles** above.

During the recruitment process: we will ensure that (except where the law permits otherwise):

- 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;
- if sensitive personal information is received, e.g. the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
- 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;
- 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
- we will only ask health questions once an offer of employment has been made.

During employment: we will process:

- health information for the purposes of administering sick pay, keeping sickness absence records, seeking legal advice, obtaining occupational health and other medical input, monitoring employee attendance and facilitating employment-related health and sickness benefits;
- sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting; and
- trade union membership information for the purposes of employee administration.

Data protection impact assessments (DPIAs)

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

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

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

During the course of any DPIA, the employer will seek the advice of the DPO for Data Protection and the views of a representative group of employees and any other relevant stakeholders.

Privacy notices

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

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.

Individual rights

Individuals (in common with other data subjects) have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notice (employees and workers);
- to obtain confirmation that an individual's information is being processed and to obtain access to it and certain other information, by making a subject access request
- to have data corrected if it is inaccurate or incomplete;
- 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');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but the individual does not want the data to be erased), or where the employer no longer needs the personal information, but the individual requires the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal information temporarily where an individual does not think it is accurate (and the employer is verifying whether it is accurate), or where an individual has objected to the processing (and the employer is considering whether the organisation's legitimate grounds override the individual's interests).

Individuals wishing to exercise these rights should contact the DPO.

Individual obligations

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

Employees may have access to the personal information of other employees, suppliers and clients of the Company in the course of their employment or engagement. If so, the Company expects that they help meet its data protection obligations to those individuals. For example, employees should be aware that they may also enjoy the rights set out in **Individual rights** above.

Employees who have access to personal information must:

- only access the personal information that they have authority to access, and only for authorised purposes;
- only allow other Company employees to access personal information if they have appropriate authorisation;
- only allow individuals who are not Company employees to access personal information if they have specific authority to do so from the DPO;
- 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 policies issued from time to time);
- 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
- not store personal information on local drives or on personal devices that are used for work purposes.

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

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions under **Sensitive personal information** being met;
- any data breach as set out under **Data breaches** below;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- 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;
- any other breach of this policy or of any of the data protection principles set out in this policy.

Information security

The Company will use appropriate technical and organisational measures in accordance with the Company's policies 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:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 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
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the Company;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the Company and under a written contract;
- the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- 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;
- the organisation will delete or return all personal information to the Company as requested at the end of the contract; and
- 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.

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 employee must seek approval of its terms by the DPO.

Storage and retention of personal information

Personal information (and sensitive personal information) will be kept securely in accordance with the Company's information security policies issued from time to time.

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. Where there is any uncertainty, employees should consult the DPO.

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.

Data breaches

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

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by an employee or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;

- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

The Company will:

- 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
- 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.

International transfers

Ordinarily, the Company does not transfer personal information outside of the UK. Exceptionally, the Company may transfer personal information outside the UK to organisations abroad 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.

Consequences of failing to comply

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

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant civil and criminal sanctions for the individual and the Company; and
- may, in some circumstances, amount to a criminal offence by the individual.

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.

Amendments to this policy

This policy is non-contractual and may be amended from time-to-time in line with changes to legislation and best practice.