Data Protection Policy

1 Employee data

This is our policy and statement of the purposes for which we hold and process personal data about our employees and others who work for us in accordance with our statutory obligations, including the EU General Data Protection Regulation ("GDPR"). We observe and abide by the Employment Practices Data Protection Code which is not enforceable by law, but which provides guidance on best practice for employers in obtaining and processing information about employees.

2 Definitions

"**Company**" means Bespoke Career Management Limited;

"data" means information which is stored either:

electronically (whether on a computer, a removable drive or any other electronic device); or
in a paper-based filing system which is structured and can be browsed by criteria, regardless of whether that filing system is dispersed across multiple locations;

"data controller" means a person (whether an individual or a corporate body) who determines the purposes for which, and the manner in which, any personal data is processed;

"data processor" means a person who processes personal data on behalf of a data controller, and does not in any way determine how or why data is processed;

"data subject" means a living individual to whom personal data relates. A data subject need not be a UK national or resident. Note that all data subjects are protected by the GDPR;

"ICO" means the Information Commissioner's Office, the UK regulator for data protection law;

"personal data" means any data (including but not limited to text, statistics, images and videos) relating to a living individual that either is identified in that data or is directly or indirectly identifiable from that data - for example only by reference to an identifier such as a name, a unique identification number, location data, an online identifier or username, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, regardless of whether that data is fact or opinion;

"processing" means any activity that involves use of personal data. It includes, but is not limited to obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties;

"sensitive personal data" means personal data that:

reveals the relevant person's race or ethnic origin, political opinions, religious or philosophical beliefs (or beliefs of a similar nature), membership of a trade union;
is genetic data, or biometric data for the purpose of uniquely identifying the relevant person;
concerns the physical health, mental health, sex life or sexual orientation of the relevant person;
relates to the commission or alleged commission of a criminal offence; or
relates to proceedings against the relevant person for a criminal offence or alleged criminal offence, including the disposal of those proceedings, or sentencing;

"security breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 General

The Company acts as a data controller, which means that during the course of our activities, we will collect, hold and process information consisting of personal data including sensitive personal data about all our employees, applicants for employment, self-employed contractors, agency workers and others who work for us. The information, which may be held on paper, within computer files or on other media is subject to certain legal safeguards in accordance with GDPR and UK domestic legislation.

This policy sets out our rules on data protection and the legal conditions which must be satisfied in relation to any act taken in relation to personal information, including but not limited to the obtaining, handling, processing, storage, transportation and destruction of personal information. Anyone processing personal data on behalf of the Company must only do so as instructed and in accordance with this policy and any other policy or procedure designed to ensure our compliance with our legal obligations.

Compliance with this policy is mandatory and non-compliance will be taken seriously and may result in disciplinary action. Employees, contractors and data processors may also have direct criminal liability, liability to the ICO and to data subjects for certain breaches under data protection laws.

If you consider that the policy has not been followed in respect of personal information about yourself or others, you should raise the matter with your line manager, the head of human resources or the chief operating officer.

4 Data Protection Principles

Anyone processing personal data must comply with six data protection principles. Those are that personal data must be:

4.1 Processed lawfully, fairly and in a transparent manner;

This includes a requirement to;

4.1.1 have a "legal basis" for processing personal data (see below);
4.1.2 be transparent with data subjects, providing them specific information about the processing to be carried out before it is carried out; and

4.1.3 to give data subjects certain rights in relation to their personal data.

When processing personal data, we must:

4.1.4 not use personal data in a way that would have an unjustified adverse effect on the individual;

4.1.5 only handle people's personal data in ways they would reasonably expect; and

4.1.6 not do anything unlawful with a person's personal data.

4.2 Collected for a specific, explicit and legitimate purpose, and not further processed in a manner that is incompatible with those purposes.
Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR or other relevant legislation.

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, or there is a new purpose, for which the data is processed, the data subject must be informed of the changed or new purpose before any processing occurs, and you must only use personal data for that changed or new purpose if it is compatible with the existing purpose.

4.3 Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

If personal data later becomes excessive in relation to the purpose, it will need to be deleted unless there is another purpose (and associated legal basis) for keeping it.

4.4 Kept accurate and, where necessary, kept up to date.

Personal data must be accurate and kept up to date. Personal data which is incorrect or misleading 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 data that cannot be rectified should be destroyed.

4.5 Kept for no longer than is necessary for the purposes for which it is processed.
Personal data should not be kept longer than is necessary for the purpose. Data should be destroyed or erased from our systems when it is no longer required for the purpose(s) originally notified to the data subject.

4.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We are must maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with our procedures and policies, or if they put in place adequate measures to ensure data security.

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

4.6.1 confidentiality means that only people who are authorised to use the data can access it;

4.6.2 integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and

4.6.3 availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central IT system instead of individual local files.

From a security point of view, only those staff listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ("database" includes paper records or records stored electronically). However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date.

In addition all employees should ensure that adequate security measures are in place. For example:

4.6.4 Restricted Areas. Any stranger seen in a non-public area should be reported;

- 4.6.4.1 Personnel files should always be locked away when not in use and when in use should not be left unattended
- 4.6.4.2 Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason
- 4.6.4.3 Destroying or disposing of personal data counts as processing. Therefore, care should be taken in the disposal of any personal data to ensure that it is appropriate. Such material should be shredded or stored as confidential waste awaiting safe destruction
- 4.6.4.4 Computer screens should not be left open by individuals who have access to personal data
- 4.6.4.5 Passwords should not be disclosed
- 4.6.4.6 Emails should be used with care
- 4.6.4.7 Care should be taken when sending personal data in internal or external mail

Any breaches of security should be treated as a disciplinary issue.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact.

A failure to observe the contents of this policy will be treated as a disciplinary offence.

5 Legal basis for processing

Personal data must be processed lawfully, fairly and in a transparent manner.

Under GDPR you must have a "legal basis" for processing. One such legal basis must apply to our processing of personal data for it to be lawful.

The GDPR allows processing for specific purposes, some of which are set out below:

5.1 the data subject has given his or her consent;

5.2 the processing is necessary for the performance of a contract with the data subject;

5.3 to meet our legal compliance obligations;

5.4 to protect the data subject's vital interests;

5.5 where the task is carried out in the public interest or in the exercise of official authority;

5.6 other than by public authorities to perform their tasks, to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy statements/notices or fair processing notices.

If processing sensitive personal data, more stringent rules apply. These include:

5.7 the data subject has explicitly consented to processing for a specific purpose (explicit consent being a clear statement in words, rather than by action);

5.8 the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the company or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or UK law;

5.9 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

5.10 the processing relates to personal data which are manifestly made public by the data subject;

5.11 the processing is necessary for the establishment, exercise or defence of legal claims; and

5.12 the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or

pursuant to contract with a health professional and subject to certain conditions and safeguards.

6 Data subject's rights and requests

Data subjects have rights when it comes to how we handle their personal data. These include:

6.1 The right to receive a copy of their personal data which the company holds; and details of:
- 6.1.1 the purpose for processing;
- 6.1.2 the categories of data processed;
- 6.1.3 any recipients (or categories of recipients) to whom the personal data has been disclosed;
- 6.1.4 the envisaged period for processing;
- 6.1.5 the existence of the right to request rectification or erasure;
- 6.1.6 the source of the information (if not from the data subject themselves);
- 6.1.7 any automated decision making, including meaningful information about the logic involved, and the significance and envisaged consequences of such decisions; and
- 6.1.8 the safeguards put in place if the personal data has been transferred outside the European Economic Area;

6.2 The right to complain to the ICO;

6.3 In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

You must immediately forward any data subject request you receive to the head of human resources whose details are listed in the appendix to this policy.

7 Right to rectification

We must rectify any inaccurate information held by us at the request of the data subject. This includes having incomplete personal data completed. This does not affect our primary obligation to keep personal data accurate and up-to-date.

8 Right to erasure*

We must erase personal data at the request of the data subject, but only in limited circumstances, namely where:

8.1 the personal data is no longer necessary for the purpose it was processed;

8.2 we originally relied on consent, that consent is withdrawn, **and** we have no other legal basis for processing;

8.3 the personal data is unlawfully processed; or

8.4 the personal data has to be erased for compliance with a legal obligation to which we are subject.

9 Right to restriction of processing

We must restrict (i.e. limit the scope of) our processing at the request of the data subject where:

9.1 the accuracy of the personal data is contested by the data subject, but only for a period enabling us to verify the accuracy of the personal data;

9.2 the processing is unlawful, and the data subject opposed the erasure of the personal data and requests the restriction of their use instead;

9.3 we no longer need the personal data for the purposes of processing, but it is required by the data subject for the establishment, exercise or defence of legal claims; or

9.4 the data subject has objected to processing pursuant to the right to object to legitimate interests processing (see below), but only pending the verification of whether our legitimate grounds override those of the data subject (if they do not, we would then have to permanently restrict processing).

10 Retention of data

The categories of information which we will hold and the minimum time for which we will normally hold it will be as follows:

Application form	Duration of employment
References received	Duration of employment
Payroll and tax information	6 years
Sickness records	3 years
Absence records	3 years
Annual leave records	1 year from end of employment
Unpaid leave/special leave records	1 year from end of employment
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
Summary of record of service e.g. name, position held, date of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

The purpose for which we hold any information about data subjects after the end of employment (as indicated in the above table) is for use solely for any residual employment related matters including but not limited to the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

11 References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' data no references (whether to prospective employers or other institutions) should be given on behalf of the Company without prior authorisation from the managing director or another director.

This policy does not prevent any employee from giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the

Company and, if the reference is given on paper, that neither the Company's name, address or logo appear on the paper.

It is our policy to provide copies of references given by us to the individual who is the subject of the reference if they request a copy.

Any requests for access to a reference given by a third party must be referred to Jimmy Bent and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore, when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However, if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymised form.

12 Reporting a personal data breach

We may be required to report personal data breaches to the ICO and in certain instances, the data subject.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the head of human resources whose details are listed in the appendix to this policy. You should preserve all evidence relating to the potential breach.

13 Human Rights Act 1998

Finally, it should be remembered that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life (Article 8)
- Freedom of thought, conscience and religion (Article 9)
- Freedom of expression (Article 10)
- Freedom of assembly and association (Article 11)
- Freedom of discrimination (Article 14)

APPENDIX

List names of those responsible for adding, amending or deleting data.

- *Jimmy Bent – Chief Operating Officer*
- *Sophie Tait – Head of Human Resources*
- *Louise Constantine – Chief Finance Officer*

List those persons responsible for responding to subject access requests.

- *Jimmy Bent – Chief Operating Officer*
- *Sophie Tait – Head of Human Resources*
- *Louise Constantine – Chief Finance Officer*