DATA PROTECTION POLICY

Issue 4 August 2018

TO ALL MEMBERS OF STAFF

Following recent changes to Data Protection rules, please find attached our updated Data Policy

INTRODUCTION

Purpose

This policy on HR data sets out our commitment to meeting our data protection obligations and to safeguarding our employees' rights in relation to their personal data that we process.

This policy applies to the personal data of employees during and after their employment with us.

The word" employee "is used throughout this policy but includes, where appropriate, workers, apprentices, interns and volunteers.

The word "employment" is used throughout this policy but may include worker, contractor or volunteer relationships, or apprenticeships or internships.

It is data relating only to the company's HR activities. We term this data "HR personal data" and refer to in shorthand as HRPD

Questions about our policy on data protection, or subject access requests, should be directed to David Ainscow, Finance Director.

The policy supplements the information already provided in our Employee handbook and in the privacy notices sent to employees.

TERMINOLOGY

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Data Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. It was previously termed "sensitive data".

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

We process HRPD in accordance with the data protection principles already well established in UK law. These are set out in full below.

- Principle 1

  Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

  a) at least one of the conditions in Schedule 2 of the Data Protection Act is met, and

  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act is also met.

- Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Principle 3

  Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Principle 4

  Personal data shall be accurate and, where necessary, kept up to date.

- Principle 5

  Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Principle 7

  Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We inform employees in our privacy notices, what data we hold; the reasons for processing that personal data; how we use such data and the legal basis for data processing. We will not process personal data of employees for any other reasons. Where we rely on our legitimate interests as the basis for processing data, we have carried out an assessment and believe that those interests are not overridden by the rights and freedoms of employees.

We will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during employment is held in the individual's personnel file in hard copy or electronic format, or both, and on HR systems. The periods for which we hold HR-related personal data are contained in our privacy notices sent to employees.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

INDIVIDUAL RIGHTS

As a data subject, employees have a number of rights in relation to their personal data.

Subject access requests

Employees have the right to make a subject access request. If an individual makes a subject access request, we will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of that data if it has been provided by the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored;
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks We has failed to comply with his/her data protection rights; and
- whether or not We carries out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to David Ainscow, Finance Director via email to davida@bentleyrowe.co.uk or in writing to our office address

We will normally respond to a request within a period of one month from the date it is received.

If a subject access request is vexatious, manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

If an employee submits such a request we will notify him/her we consider this to be the case.

An employee may raise a grievance under the Company's procedure is he/she disagrees with our decision.

OTHER RIGHTS

Employees have a number of other rights in relation to their personal data. They can require us to:

- make corrections to inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual withdraws consent:
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override our legitimate grounds for processing data.

To ask us to take any of these steps, the individual should send the request to David Ainscow, Finance Director.

DATA SECURITY

We take the security of HRPD seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by authorised employees in the course of their employment.

Where we share your personal data with third parties or engage them to process data on our behalf, such parties are under a duty of confidentiality and are obliged to Implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

We do not consider that any of the processing we carry out would result in a high risk to privacy such as to require us to conduct an impact assessment.

DATA BREACHES

If we discover that there has been a breach of HRPD that poses a risk to the rights and freedoms of Employees, we will report it to the Information Commissioner within 72 hours of discovery. All data breaches are recorded regardless of their effect.

International data transfers. We do not transfer HR-related personal data to countries outside the EEA.

INDIVIDUAL RESPONSIBILITIES

Employees are responsible for helping us keep their personal data up to date.

You should let us know if data provided to us changes, for example if you move house or changes bank details.

Employees who have access to the personal data of other employees and of our customers and clients in the course of their employment. Where this is the case, we require you to help us meet our data protection obligations.

Employees who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to employees who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data in any format from our premises without authority and then only in accordance with our rules or removing data
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to David Ainscow, Finance Director immediately.

A failure to comply with the data protection rules associated with your employment would constitute a disciplinary offence and in cases where the breach has been flagrant and deliberate or a result of gross negligence, with potentially serious consequences for other employees or our customers, the penalty may be dismissal.

Training. We provide training to all Employees commensurate with their data protection responsibilities. Should you wish to discuss any of the above, please do not hesitate to contact me, David Ainscow, Finance Director.