DATA PROTECTION

Data protection compliance should be seen as an integral part of employment practice. It is important to develop a culture in which respect for private life, data protection, security and confidentiality of personal information is seen as the norm.

SCOPE

The company is fully committed to ensuring compliance with the requirements of the General Data Protection Regulation ("the regulation"), and regards the lawful and correct treatment of personal data as important to its successful operations and maintaining confidence between us and those with whom we interact.

Additional policies and procedures have been established to ensure that all employees who have access to any personal data held by, or, on behalf of us are fully aware of, and abide by their duties under the regulation.

This policy applies to all employees.

RESPONSIBILITY

Knights Brown has a data protection office at Head Office, 160 Christchurch Road, Ringwood BH24 3AR. Whilst we do not have a data protection officer, the following individuals ensure the right systems, procedures and training are in place to support the compliance of the regulation:

- Sarah Whittle, HR Manager 01425 482295
- Peter Williamson, Business Systems Director 01425 482298

The email address for contacting the office with regards to data protection is:

- data.protection@knightsbrown.co.uk

All our employees should be aware of and work within their responsibilities for the personal data they hold about an individual.

In addition, heads of department must ensure their departments are fully aware of the personal data they hold and how they should process it.

DATA

Data is information which is stored electronically, or in paper based filing systems.

Personal Data is any data relating to a living person, who can be identified through this data. This can be a personal email address, home address, date of birth, habits, lifestyle, computer IP addresses, education, and includes any expression of opinions about that person such as that held in probation reviews, PDRs.

Special Category Data: This data is sensitive personal data about the individual such as:

- Physical or mental health
- Sexual orientation
- Racial or ethnic origin
- Political opinions
- Religion or Beliefs
- Trade union membership

In addition, while criminal record checks are separately categorised under the regulation they are treated in a similar way due to the sensitivity of this data.

INDIVIDUAL RIGHTS PROTECTED UNDER THE REGULATION

- The right to be informed
- The right to access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to object
- The right to data portability
- Rights in relation to automated decision making

The documents listed below provide further advice on the personal data we hold as a company, why we hold it and what we do with it, and gives advice with regards to the individual rights listed above. The documents will assist our employees in processing personal data correctly.

- Data Protection Guidance Notes
- Privacy Notice
- Data Retention Policy

REPORTING BREACHES

Any breaches of the regulation, whether deliberate or not, should be reported to the human resources manager or the business systems director without delay on the contact details above. This will enable all necessary measures to be put in place to minimise and mitigate any breaches. Information should include as much factual information as possible as to the breach that has taken place.

We encourage all those who have any concerns about how personal data is being processed, whether a breach has been made or not, to discuss this matter further. This will ensure any proactive measures such as training or procedural changes can be instigated and can prevent potential future breaches.

Any deliberate and malicious breach of an individual's personal data will lead to disciplinary action being undertaken.

Our data breach policy provides details on how to report a breach as well as the company's response plan.

SUBJECT ACCESS REQUEST

Under the regulation, an individual can request access to personal information about themselves, which is controlled by the company. To do this you should email the data protection office on the email address above, ideally with sufficient detail to enable the data to be identified.

The HR and IT departments will be responsible for processing 'subject access requests' within one month from receipt of request. For more complex requests the company may advise the individual that they need to extend this period and may charge an administration fee.

STAFF TRAINING

All staff who process personal data will be required to undertake an e-learning course to understand their responsibilities. Key job holders and heads of department are required to undertake a more detailed e-learning programme based on the role that they undertake.

This policy does not form part of the contract of employment and may be amended by the company from time to time.

MAY 2018