Job Applicant Privacy Notice

Please Note:
The wording in this document reflects the requirements of the General Data Protection Regulation (GDPR) which came into effect in the UK on 25 May 2018.

Data controller: Andrew Beale, c/o Beales Hotels Ltd, West Lodge Park Hotel, Cockfosters Road, Hadley Wood, Herts, EN4 8LH, Tel. No. 020 8216 3900.

As part of any recruitment process, Beales Hotels ('the organisation') collects and processes personal data relating to job applicants, and individuals on Work Experience Placements / Internships. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects a range of information about you. This may include:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief
- Information related to an individual's Work Experience/Internship, incl. personal contact details, Next of Kin details, info. about career aspirations, related Risk Assessments etc.

The organisation collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment (including online, electronic, paper tests, in-tray exercises, working trials or assessment centres etc.)

The organisation will also collect personal data about you from third parties, such as Recruitment Agencies who may be representing you, references supplied by former employers, information from employment background check providers and information from criminal records checks (as/when appropriate/required), information from your school / College or place linked to your education etc. With the exception of Recruitment Agencies and organisations linked to your education who are representing you, the organisation will only seek information from third parties once a job or placement offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR and H&S files, in management systems and on other IT systems (including email).

Why does the organisation process personal data?
The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements, or to administer your Work Experience placement / Internship etc.
In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. (For certain positions, it is

necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.)
In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- For Health and Safety and company procedural reasons, to comply with any Regulations / guidelines etc. during Work Experience placements/internships (if applicable).
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and Payroll, T&D and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.
Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). If/when information about trade union membership is processed, this is to allow the organisation to operate check-off for union subscriptions.
Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

Who has access to data?
Your information will be shared internally, including with members of the HR, Payroll/Accounts and Training & Development Team, your line manager, managers in the business area in which you work, Senior Management and IT staff *if access to the data is necessary for performance of their roles*.

The organisation shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers (and obtain necessary criminal records checks from the Disclosure and Barring Service, if required), plus specified individuals at School/College/place of education for Work Experience/Internships. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.
The organisation may also share your data with third parties that process data on its behalf in connection with payroll, the provision of benefits and the provision of occupational health services.

The organisation will not transfer your data to countries outside the European Economic Area.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. This includes:

- Data stored in securely in locked cupboards, cabinets, files etc. at Head Office, in HR Office, and in designated storage areas at both Hotels, with restricted access to specified and approved individuals only
- Keys to storage areas containing personal and sensitive data are only assigned to or available to be used by specified and approved individuals only and are stored safely in relevant ways including in key cabinets etc.
- spreadsheets and databases containing Personal Data and Sensitive data are stored safely on hotel HR, Payroll and Business systems and files/records, with restricted access to specified and approved individuals only and with additional password protection/similar as required.
- Personal devices which may hold or have capability to access personal or sensitive data are used, transported and stored in an appropriate way that is in line with achieving and maintaining highest levels of data security. E.g. Personal / company mobile phones have pin codes which are not shared with others and are changed as required, laptops have password protected access and are not left unattended or stored in vehicles overnight, etc. Passwords/pins etc. are not shared with anyone other than the staff they have been assigned to, or other specified staff authorised to have access).
- Any documents or data no longer required or which contain personal and/or sensitive information, sensitive policy / company information etc. will be destroyed in line with appropriate security procedures, e.g. made either unreadable, or unreconstructable as required (following the retention periods specified), including: by electronic shredding, incineration, physical disks and media being subject to a secure wipe or disposed of, CDs, DVDs to be destroyed etc.
- All staff are required to comply with the organisations security and confidentiality policy, and they also have statutory requirements to comply with regarding maintaining data confidentiality; this will include staff and guest personal data and sensitive data that they have access to, see/hear, process, record etc.
- There are specific systems restrictions in place which would not allow access to certain unauthorised/unapproved/inappropriate websites, systems etc. from the organisations computers/systems etc. which are put in place by the organisations IT providers.
- The organisation consults with and uses the services of IT specialists, who assist the organisation to implement, monitor and maintain the highest levels of IT security in line with business needs and the requirements of the GDPR.

Where the organisation engages third parties to process personal data on its behalf (e.g. for Pensions and Insurance processes/services etc.), such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

The organisation will hold your personal data relating to the recruitment process as follows:

Documents / Data	***Retention Period***
Application forms, CVs and interview notes (for unsuccessful candidates) and other information / data relating to and gathered during the recruitment process	3-6 months from the end of the recruitment process.
Basic personnel information e.g. name, contact details incl. telephone number, email address etc. (for unsuccessful candidates)	3-6 months from the end of the recruitment process.

Right to work documents incl. Passports (for unsuccessful candidates).	3-6 months from the end of the recruitment.
Personal info./data relating to your application for Work experience etc.	Up to 6 years from end of Work Experience / Internship

N.B. Information about data retention period for successful candidates will be outlined in the organisation's Employee Privacy Policy.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Andrew Beale, in writing, c/o Head Office, at West Lodge Park Hotel, or email headoffice@bealeshotels.co.uk

If you want to make a subject access request regarding your data, this can be done by completing the organisation's Subject Access Data Request Form. The form can be requested via email to the Data Controller, Andrew Beale, c/o email: headoffice@bealeshotels.co.uk , and will need to be completed by you and returned to Andrew Beale at either one of the above postal/email addresses.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.