Privacy Notice for Job Applicants

Brighter Places is committed to ensuring that the privacy of everyone whose personal data it collects is protected. All the personal data we collect and process is used in accordance with the UK GDPR and the Data Protection Act 2018.

This Privacy Notice sets out why we collect personal information for job applicants, how we use it and who we may share it with. It also explains individuals' rights under the UK GDPR. If we ask for information which can be used to identify an individual, we will only use it in accordance with this Privacy Notice.

Brighter Places as the data controller

Brighter Places is a data controller, meaning that it determines and implements various processes for how it uses personal information.

Our contact details are:
E-mail: dataprotection@brighterplaces.co.uk

Post: Data Protection Officer, Brighter Places, Eden House, Eastgate Office Park, Eastgate Road, Bristol BS5 6XX

The information we collect from job applicants

We may hold different categories of data about job applicants and employees, including:

- Personal details, including name, address, date of birth, nationality, email address and phone numbers
- Information related to special category data (e.g. medical information) if it has been asked for and provided
- Information included in application forms or CVs including education history, employment history, references, training qualifications or courses
- Documentation relating to the right to work in the UK
- Driving licence details
- Information relating to potential conflicts of interest (if relevant)
- information relating to criminal convictions (if relevant)

How and why we collect job applicants' data

We collect data in a variety of ways including the information included in application forms or CVs either direct or from recruitment agencies and the equal opportunities monitoring form we ask job applicants to complete.

Notes made by our recruiting officers during the applicant selection process are also retained in line with our Data Retention Schedule.

We may also collect and retain other data that will help us to fulfil our legal obligations. To ensure we treat all job applicants and employees fairly and equally, it is important that we have on file information about individuals' disabilities or other specific needs.

All job applicants' and employees' personal data is securely stored in the Human Resources, Finance, and IT filing systems.

How we use job applicants' personal information

We collect and retain personal information, which may sometimes include special category data, so that we can provide a recruitment service.

For job applications these are:

- to perform the employment contract that we enter into with our employees
- to carry out any duties required by law for recruiting and employing staff
- to protect our job applicants' and employees' interests
- to ensure we always act in the public interest.

We can claim legitimate interest for processing job application data because:

- we can reasonably be expected to process personal information for staff recruitment and employment purposes
- we ensure that the processing has minimal impact on privacy
- there is a compelling justification for processing the data

'Special category' data

Under the UK GDPR, certain personal information is classed as 'special category' data. This includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data about sexual orientation.

In many situations it is not necessary for us to gather this information, but where we do need it we minimise the collection and use of special category date and personal information.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of certain roles and where the law permits us. This data will usually be collected at the recruitment stage, but may also be collected during employment.

We use criminal conviction data to comply with Disclosure and Barring Service (DBS) requirements for certain roles.

To allow us to process this data, we rely on the lawful basis that the nature of the work involved in some positions may bring employees into contact with vulnerable people and/or information about vulnerable people when processing data.

Consent

Applicants have the right to withdraw their consent for us to use their data at any time but it is important to note that if we do not have permission to process personal data, for example where we are required to confirm the right to work in the UK or, where appropriate, carry out a DBS criminal convictions check, we may be unable to progress job applications.

Sharing personal information within BP and other organisations

Personal data will be shared with colleagues within Brighter Places where it is necessary for them to undertake their duties with regard to staff recruitment. This includes, for example, the Human Resources department, those in the department where the vacancy is situated and the IT department, who arrange access to our systems and payroll bureau.

In some cases we collect data from third parties such as employment agencies, and data may also be shared with third parties such as previous employers to obtain references when applications are successful.

Protecting personal data

We are committed to ensuring that personal information is stored securely. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect, process and share.

We use external service providers who handle your personal information on our behalf. We have appropriate agreements in place with these service providers.

Where a service provider is located outside the UK, we make sure any transfers of personal information are protected by an adequacy decision, or other appropriate safeguards measures, such as Standard Contractual Clauses.

How long we keep personal information

In line with data protection principles, we only keep applicants' data for as long as we need it. These retention periods are documented in our Data Retention Schedule and will depend on whether or not the applicant was successful in obtaining employment with us.

If applicants are unsuccessful in obtaining employment with us, we will seek their consent to retain their data for 12 months after the recruitment period has ended in case other suitable job vacancies arise within Brighter Places for which we think they may wish to apply. Consent may be withheld or withdrawn at any time.

If we have not sought consent, or consent has not been given, to keep personal data on file for the purpose of future suitable job vacancies, we will retain it for 6 months after the recruitment exercise has ended.

At the end of the retention period, we will delete or destroy the data, unless consent has already been withdrawn, in which case it will already have been deleted or destroyed.

Successful applicants' data is kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which is provided when they start work.

Individuals' rights in relation to personal data

The UK GDPR gives certain rights to individuals in relation to the personal data we hold and process. These include:

- *The right to be informed*
    - Individuals have the right to be informed about Brighter Places' purposes for processing their personal data, how long Brighter Places will retain that data, and who Brighter Places will share it with. This information is provided in this Privacy Notice.

- *The right of access:*
    - Individuals have the right at any time to ask what information we hold about them and how we use it. This is called a Subject Access Request (SAR). A SAR can be made verbally to a Brighter Places employee by phone or in writing. We may request proof of your identity.

      We will respond to all SARs within one month. We are permitted to extend the time to respond by a maximum of a further two months if a request is particularly complex or a number of different requests have been made by a single individual. We will contact the individual within one month of receiving their request to explain why the extension is necessary.

- *The right to rectification*
    - Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

- *The right to erasure*
    - Individuals have the right to have personal data erased, also known as 'the right to be forgotten'. However, in some instances we may have to retain data for specified purposes. Each situation will be reviewed on a case by case basis and if we need to refuse a right to erasure request we will explain the reasons why.

- *The right to data portability*
    - Individuals have the right to data to obtain and reuse their personal data for their own purposes across different services; to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

- *The right to object*
    - Individuals have the right to object to the processing of their personal data in certain circumstances.

- *The right to restrict processing*
    - Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
    - When processing is restricted, organisations are permitted to store the personal data, but not use it.

- We reserve the right in some cases to continue to use personal data if we are legally obliged to and/or where we consider processing to be necessary and can claim a lawful basis or legitimate interest for doing so.

- *Rights in relation to automated decision making and profiling*
  - Individuals have the right to object to automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual).
  - Brighter Places does not carry out automated decision making or profile data.

To exercise any of the rights explained above, please contact our Data Protection Officer:

E-mail: dataprotection@brighterplaces.co.uk

Post: Data Protection Officer, Brighter Places, Eden House, Eastgate Office Park, Eastgate Road, Bristol BS5 6XX

Information Commissioner's Office (ICO)

The ICO is the supervisory authority in the UK for data protection matters.

More information about the UK-GDPR, individuals' rights and how to assert them and information about how to make a complaint is available from the Information Commissioner's Office (ICO).

The ICO's website is at https://ico.org.uk/

Questions about Brighter Places' Job Applicants' Privacy Notice

We are happy to answer any questions or provide a copy of our full Data Protection Policy on request.

E-mail: dataprotection@brighterplaces.co.uk

Post: Data Protection Officer, Brighter Places, Eden House, Eastgate Office Park, Eastgate Road, Bristol BS5 6XX