



Applicant Privacy notice

Bricks collects and processes personal data relating to individuals who apply to work for the organisation so that we can manage the recruitment process. We are committed to being transparent about how we collect and use that data, and to meeting our data protection obligations.

What information does Bricks collect?

Bricks collects and processes a range of information about you. This includes:

1. your name, address and contact details, including email address and telephone number, date of birth and gender;
2. details of your qualifications, skills, experience and employment history, including suitability for working with children and young people, start and end dates with previous employers/other organisations whom you have worked for (in an capacity);
3. information about your nationality and entitlement to work (whether paid or unpaid) in the UK;
4. information about your criminal record;
5. details of your hours of availability;
6. training you have participated in, and related correspondence;
7. information about medical or health conditions, including whether or not you have a disability for which Bricks needs to make reasonable adjustments;

Bricks collects this through application forms, CVs, your passport or other identity documents such as your driving licence; forms completed by you at the start of or during our relationship; from correspondence with you or through interviews, meetings or other assessments.

In some cases, Bricks collects personal data about you from third parties, such as references supplied by former employers, or other organisations with whom you have worked for (in any capacity) information from background check providers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personal file in Bricks's HR and management systems and in other ICT systems (including Bricks's email system).

Why does Bricks process personal data?

We need to process data to follow Safer Recruitment and Safeguarding requirements and ascertain your suitability for any roles you apply for with Bricks.

In other cases, Bricks has a legitimate interest in processing personal data before, during



and after the end of the relationship. Processing individual data allows us to:

1. run recruitment and promotion processes;
2. maintain accurate and up-to-date records and contact details;
3. operate and keep records, to ensure acceptable conduct within the organisation and workforce management purposes;
4. obtain medical information to ensure that we comply with duties in relation to individuals with disabilities, meet obligations under health and safety law;
5. ensure effective general HR and business administration;
6. respond to and defend against legal claims; and
7. maintain and promote equality across the organisation

Where Bricks 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 individuals or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out legal obligations (such as those in relation to individuals with disabilities and for health and safety purposes).

Who has access to data?

Your information will be shared internally, including with members of the HR and recruitment team and managers in the business area in which you have applied for work,

Bricks shares your data with third parties in order to obtain references from other employers, or organisations you have worked for in any other capacity to obtain background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

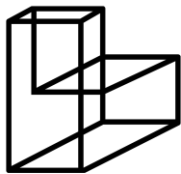
Bricks may also share your data with third parties that process data on its behalf, in connection with the provision of safeguarding and HR services.

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

How does Bricks protect your data?

We take the security of your data seriously. Bricks 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 or representatives in the performance of their duties for the organisation. Data stored is password protected and hard drives are encrypted. Strict access controls are implemented to ensure that only those with permitted access are able to access the relevant data.

Where Bricks engages third parties to process personal data on its behalf, they do so on



BRICKS

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 Bricks keep data?

Should you be successful in your application, we will hold your personal data for the duration of your retention by Bricks. The periods for which your data is held after the end of your retention are 6 years. Data relating to checks made with the Disclosure and Barring Service are retained for 7 years. Details relating to unsuccessful applications to work at Bricks in any capacity are retained for 12 months.

Data held for unsuccessful applicants will be securely disposed of after six months. Bricks cannot save applications with the intention of considering them for future positions. Should you wish to express an interest in applying for work with Bricks after having submitted a previous, unsuccessful application for work with Bricks (in any capacity), you will be required to submit a new CV and application form.

Your rights

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

1. access and obtain a copy of your data on request;
2. require Bricks to change incorrect or incomplete data;
3. require Bricks to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
4. object to the processing of your data where we are relying on our legitimate interests as the legal ground for processing; and
5. ask Bricks 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.

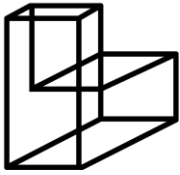
If you would like to exercise any of these rights, please contact Bricks's Data Controller, Susan Parry, by emailing: Susan@bricksbristol.org

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

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide your data to Bricks during the application and recruitment process, however, if you choose not to provide the information requested, we may be unable to process your application.

Automated decision-making



BRICKS

Recruitment decisions in respect of unpaid work for the organisation are not based solely on automated decision-making.