Privacy Notice for Job Applicants

About The Forbury Clinic

The Forbury Clinic is the trading name of Berkshire Health Limited, registered office Wilson House, Waterberry Drive, Waterlooville, Hampshire, United Kingdom, PO7 7XX. Company Registration Number 07238700. Registered in England & Wales.

Berkshire Health Limited (BHL) is registered with the Information Commissioner's Office, registration number Z274620.

Introduction

This privacy notice is for people who have applied, or are considering applying, for a job as an employee, worker, contractor or volunteer at BHL.

BHL is a wholly owned subsidiary of Genesis Cancer Care UK Limited (GenesisCare) and for the purposes of data protection legislation BHL and GenesisCare jointly control your data.

This Job Applicant Privacy Notice describes how we collect and use your personal data for the purposes of the recruitment and onboarding process and how long it will be retained for. It provides you with certain information that is required under the General Data Protection Regulation (GDPR).

A separate Staff Privacy Notice will be made available for applicants who successfully complete our recruitment process.

Our recruitment process includes partnering with trusted agencies with whom we have an existing relationship and who understand our values. Applications are generally received through our website which is linked to our People Management system – Workday – and are evaluated against the role requirements. If we decide to call you for an interview we will use the information you have given us at the interview to decide whether to offer you the role. If the role is offered by us and accepted by you we will take up references and, where relevant, carry out a Disclosure and Barring Service (DBS) check and occupational health screening before confirming your appointment. If you are unable to provide the information we require, such as evidence of qualifications, work history, relevant references and right to work documentation, we will not be able to process your application successfully.

The type of personal data we handle

In order to carry out our recruitment activities and obligations we handle personal data and special category personal data.

Personal data means any information relating to an identifiable person who can be directly or indirectly identified, for example identified by a name, a reference number, address, date of birth, etc.

Special category personal data is information about an individual's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, sex life or sexual orientation and health, including genetic and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to the processing of such data.

How we obtain your data

Data about you is provided from the following sources:

- Directly from you
- From an employment agency
- CCTV images taken using our own CCTV systems in certain settings
- From security clearance providers
- From our occupational health provider
- Your named referees and previous employers
- From your employer relating to TUPE (transfer of undertaking of protection of employment)
- Data from third parties that is from a publicly accessible source, such as proof of professional registrations where applicable.

How we will use your personal data

We will use the personal information we collect about you to:

- Communicate with you about the recruitment process
- Assess your skills, qualifications and suitability for the role
- Carry out background and reference checks, where applicable
- Keep records related to our recruitment processes
- Comply with legal or regulatory requirements.

How we will use your special category personal data

We will use the special category personal information we collect about you to:

- Consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview
- Ensure meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

We will collect information about your criminal convictions history when you are offered a role that requires a basic, standard or enhanced DBS check in accordance with Disclosure and Barring Service guidance. For certain roles it is a statutory requirement. The purpose is to satisfy the organisation that there is nothing in your criminal convictions history which makes you unsuitable for the role. We process data about criminal convictions and offences in accordance with data protection legislation.

Data processed at the application and offer stages

The tables below describe the data we handle and what we need it for. It also explains the basis we can rely on to request and retain data about you.

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter
- The information you have provided on an application form, including (but not limited to) name, title, address, telephone number, personal email address, date of birth, gender, employment history, and qualifications, if provided
- Any information you provide to us during an interview.

The data that we handle in relation to job applications	**What we need it for**	**Why we process it, i.e. the lawful basis**
Your name, address, personal e-mail address, telephone number(s)	To contact you, to respond to your queries and make any interview arrangements with you	It is in our legitimate interests to decide whether to appoint you to the role or provide you with work since it would be beneficial to our business to appoint someone to that role or work
Details of your qualifications, skills, experience and employment history, including start and end dates with previous organisations	To assess your job application and suitability for the role	We have a legitimate interest in processing your data to decide whether to enter into a contract of employment or work with you
Details of role applied for and salary expectations	To ensure we are matching applicants' expectations to the roles and salaries we have available	We have a legitimate interest in ensuring high user engagement and experience
Online behavioural and cognitive profiles	To assess the organisation's alignment with the interests and characteristics of the applicant	It is in our legitimate interests to consider the organisation's culture and evaluate the best match of applicant and role
Images of you on our CCTV network in certain settings, for example, at the location where you attend an interview	For protection and crime prevention	We have a legitimate interest in protecting our staff, patients and the public by using CCTV on our premises

If you are offered a role with us we will collect, store and use the following additional personal information:

- Proof of your identity and the information you have provided to us
- Information about your health, including any medical condition
- Information about criminal convictions and offences.

The data that we handle in relation to job offers	**What we need it for**	**Why we process it, i.e. the lawful basis**
Documentation confirming your right to work in the UK which will include passport details, date of birth, gender	To check you are legally entitled to work in the UK	We have a legal obligation to perform these checks
Criminal convictions and offences (including alleged offences) as detailed in a criminal record check. This may include details of criminal proceedings, outcomes and sentences. Applies only to roles where a criminal record check is a condition of employment	To help us employ the right people for certain types of work, for example, working in certain healthcare settings	We have a legal obligation to perform DBS checks for certain types of role
References (received from a third party)	To support the organisation in making appointment decisions about you	We have a legitimate interest in obtaining references from previous employees prior to making a firm offer of employment
Statutory and voluntary registration data, where required, to include qualifications and professional memberships	To ensure you hold the necessary certification, qualification or professional memberships	We have a legitimate interest in seeking assurance of necessary qualifications prior to making a firm offer of employment
Data about any medical or health conditions you may have	To assess your fitness for the role and any requirement for reasonable adjustments	We have a legal obligation to ensure that we provide reasonable adjustments in line with the Equalities Act 2010
A copy of your offer letter, your contract of employment and job description	To offer you a role or work in our organisation	To comply with legal obligations in relation to employment

Data sharing

Your information may be shared internally for the purposes of the job application exercise. This includes members of the GenesisCare People & Culture team, relevant managers and interviewers involved in the recruitment process. Our online behavioural and cognitive profile system provider will have access to data such as your name, email address and job role and be bound by a contract with standard data protection clauses; further information is provided when accessing the system.

We will not share your data with third parties unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you and employment background check providers to obtain necessary background checks, as described above.

International transfers of your personal information

We are part of a global organisation and we (or third parties acting on our behalf) may store or process personal information within the GenesisCare group of companies for administrative and management purposes. The group companies are located in Spain and Australia and the United States. This processing is based on our own or a third party's legitimate business interests.

As a global organisation GenesisCare may engage global suppliers for the provision of services to the GenesisCare group of companies and such suppliers may also be located outside the UK.

Where we transfer your personal data to a third country or international organisation, we will ensure adequate safeguards and measures are in place to protect your personal data from unlawful use and ensure your fundamental rights are capable of being upheld. We would normally achieve this by:

- Only transferring personal data to countries deemed capable of providing an adequate level of protection; or
- Implementing Standard Contractual Clauses; and
- Adopting technical, organisational and contractual measures, where required

In certain situations, it may be possible to legitimise the transfer by relying on a derogation. For example, if:

- You have explicitly consented to the proposed transfer; or
- The transfer is necessary for the performance of a contract

In all cases any transfer of your personal information will be compliant with applicable data protection law. If you would like further information regarding the steps we take to safeguard your personal information when making international transfers, please contact the DPO using the details at the foot of this Privacy Notice.

Data security

Your data may be stored within electronic or paper records, or a combination of both. Under the General Data Protection Regulation/Data Protection Act 2018 strict principles govern our use of data and our duty to ensure it is kept safe and secure. We have put in place appropriate

security measures to protect your personal information and we limit access to your data to those persons who have a business need-to-know. Everyone working for GenesisCare is subject to the common law duty of confidentiality. This means that any data you provide to us in confidence will only be used in connection with the purpose for which it was provided, unless we have specific consent from you or there are other special circumstances covered by law. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

How we will secure your personal data

We take privacy seriously and will ensure your personal data is appropriately secured and protected from being accidentally or deliberately compromised.

Those staff members managing the P&C function are trained to handle your data correctly and to protect your confidentiality and privacy.

We maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your data is never collected or sold for direct marketing purposes.

Technical and organisational measures we take to ensure the security of your information include:

- An established network of individuals across the organisation who are accountable and responsible for information risk management
- Existence of various organisational measures including policies and procedures, providing regular training in handling personal data lawfully and conducting regular compliance checks
- Lockable rooms, cabinets, individual log in credentials, encryption and secure disposal of confidential waste
- Ensuring only appropriate individuals have access to relevant and proportionate information about you
- Restricted access to electronic systems and folders
- Carrying out checks on third parties who process personal data on our behalf.

Data retention

If you are not successful in your application we will retain your personal data for a minimum period of six months and a maximum period of one year. Data will be managed and disposed of in an appropriately secure manner.

If we wish to retain your personal information on file, on the basis that a further suitable opportunity may arise in future, we will seek your explicit consent to retain your personal information for a fixed period on that basis.

Successful job applicant documentation will be transferred to the organisation's HR system and information in relation to the processing of your data as an employee will be provided to you in a separate privacy notice.

Rights of access, correction, erasure, and restriction

Under certain circumstances you have the right to:

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are processing it lawfully.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below). There may be a legal or other reason why we need to retain your data. If this is the case we will tell you.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party. This right will not apply in GenesisCare job application scenarios as data portability only applies where the lawful basis for processing is consent or for the performance of a contract and processing is by automated means.
- **Automated decision-making:** You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making in GenesisCare job application scenarios.

Updates to this Privacy Notice

We may update this Privacy Notice from time to time to ensure that it remains accurate. In the event that these changes result in any material difference to the manner in which we process your personal data we will signpost you to the specific changes.

Information Commissioners Office (ICO)

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, for example if you are unhappy with the way that we have dealt with a request from you to exercise your rights, or if you think we have not complied with our legal obligations.

Whilst you are not obliged to do so, we would appreciate you making us aware of any issue prior to notifying the ICO and giving us the opportunity to respond. Please contact the BHL DPO whose details are at the foot of this privacy notice.

Making a complaint will not affect any other legal rights or remedies that you have.

Information Commissioner's Office, at casework@ico.org.uk, or at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or telephone 0303 123 1113 (local rate call). Website: https://ico.org.uk/

Questions and queries

If you have any queries or would like to exercise your rights or to establish whether any rights apply to you, please contact:

- Your recruitment manager, or
- Abby Morgan, Clinic Manager: 23 Craven Road, Reading, RG1 5LE, or email abby.morgan@theforburyclinic.co.uk, or

Data Protection

If you have any questions about this privacy notice or how we handle your personal data please contact the DPO:

Data Protection Officer: BHLdpo@genesiscare.co.uk or telephone 07956 616 414