GPS Healthcare

GDPR PRIVACY NOTICE

Applicants (Recruits)

GPS Healthcare is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

1. Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

2. The kind of information we hold 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 covering letter, curriculum vitae, application form and speculative application forms including name, title, address, telephone number, personal email address, date of birth, gender, employment history, education, professional membership, qualifications, NI number and referees.
- Any information you provide to us during an interview.
- A record of interview questions and scoring results
- Microsoft office test results and presentations.
- Applicants who are successful and offered the appointment will also have the following ID collected for the purpose of pre-employment checks.
- Right to work documentation (passport)
- Address Confirmation (in the form of two official documents)
- DBS checking documentation (including full name, date of birth, passport, driving licence, birth certificate, marriage certificate, proof of address and confirmation of periods of residency over 5

years, NI number).

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

3. How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Recruitment agencies that you may have applied through.
- Complete Background Screening (CBS) background check provider for the Disclosure and Barring service in respect of criminal convictions.
- The British Medical Journal
- NHS Jobs
- Employment services provider (for example total jobs)
- Training Programmes e.g. key training and colleges.
- Your named referees, from whom we collect the following categories of data: the capacity in which the referee has known the candidate i.e. on a personal or professional level, over what period of time, the start date and end date of their employment, the position held at the time of their employment, confirmation of hourly rate/salary, the candidates suitability for the post, any concerns raised regarding the candidates clinical practice, the candidates time-keeping, reliability and ability to work as part of a team, sickness absence record, reason for leaving current role and any other general comments.
- The following data from third parties is from a publicly accessible source Nursing and Midwifery Council (NMC), General Medical Council (GMC), General Pharmaceutical Council (GPhC), National Medical Performers List Confirmation.

4. How we will use information about you

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

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

It is in our legitimate interests to decide whether to appoint you to role/work since it would be beneficial to our business to appoint someone to that role/work.

We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your CV, covering letter and/or your application form we will then process the information through a shortlisting process to decide whether you meet specification requirements. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to invite you for an interview, we will use the information you provide to us at the interview and test/presentation results where applicable to decide whether to offer you the role/work. If we decide to offer you the role/work, we will then take up references **and** ask you to supply us with the necessary data to carry out a criminal record check, right to work checks, address confirmation and qualification certificates if applicable. For medical applicants we will also complete professional membership checks through the General Medical Council (GMC), Nursing and Midwifery Council (NMC), General Pharmaceutical Council (GPhC), and National Medical Performers List Confirmation before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, we require a DBS check and references for this role and failure to provide us with relevant details to allow us to carry out these checks will result in us being unable to take your application further.

5. How we use particularly sensitive personal information

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status 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 **OR** through any other stage of the recruitment process.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
  We will use your information to carry out DBS checks to ensure safe recruitment.

6. Information about criminal convictions

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you the work/role. We are required to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- We are legally required by Care Quality Comission (CQC) to carry out criminal record checks for those employed by GPS Healthcare.
- All roles within GPS Healthcare require a high degree of trust and integrity. Administration roles may require employees to work on an individual basis with vulnerable adults and children. For the safeguarding of patients and staff in line with GPS Healthcare DBS Policy, administration roles undergo an enhanced with barred lists check from the Disclosure and Barring Service.
- Clinical roles involve working directly with vulnerable adults and children. For the safeguarding of patients and staff in line with GPS Healthcare DBS Policy, clinical roles undergo an enhanced with barred lists check from the Disclosure and Barring Service.

We have in place an appropriate policy document (our DBS Policy) and safeguards which we are required by law to maintain when processing such data.

7. Automated decision making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

8. Why might you share my personal information with third parties?

We will only share your personal information with the following third parties at the stage of a successful application and your acceptance of appointment for the purposes of moving your application to the pre-employment check stage.[Third parties that we will share personal information with include:

- Complete Background Screening (CBS) (for the purpose of DBS Checks)
- NHS Midlands and Lancashire Commissioning Support Unit (for IT purposes)
- Care Identity Service (for smartcard purposes)
- Laboratory Medicine Information System Heart of England NHS Foundation Trust (for pathology access)
- ICT Service, Heart of England NHS Foundation Trust (for ICare access)
- Solihull Clinical Commissioning Group (for prescribing codes)
- Primary Care Support England (PCSE) (for National Medical Performers Lists)

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

9. Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Data Protection Officer.

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.

10. Data Retention

How long will you use my information for?

We will retain your personal information for a period of 12 months after we have communicated to you our decision about whether to appoint you to the role/work. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with [our data retention procedure.

For applicants who are successful at the recruitment stage, please refer to GPS Healthcare Privacy notice for employees, workers, contractors.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

11. Rights of access, correction, erasure and restriction

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information 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 information. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information 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. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the

processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Business Manager in writing.

12. Right to withdraw consent

When you applied for this role, we provided you with this privacy notice and you confirmed consent to us processing your personal information for the purposes of the recruitment exercise. You have the right to withdraw your consent for processing of your data at any time. To withdraw your consent, please contact the Data Protection Officer by email recruitment.gps@nhs.net Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely.

13. Data Protection Officer

We have appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection officer by email recruitment.gps@nhs.net. 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.