

Job Applicant Privacy Notice

Version:	Review date:	Edited by:	Approved by:	Comments:
1	17.06.19	JAC	LH	New document
2	14.10.19	JAC	LH	Amended to meet new legislation
3	27.05.21	JAC	LH	Amendment re access and complaint

Data controller: Dr Smithson

Data protection officer: Amanda Holloway CAPCCG.DataProtectionOfficer@nhs.net

The Practice gathers and processes personal data of job applicants as part of the recruitment process. We are committed to being open and transparent about how we gather and use that data and to meeting our data protection obligations.

Collecting information

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of your employment history, skills and experience;
- your contact details and date of birth;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the Practice needs to make reasonable adjustments during the recruitment process;
- information in relation to your right to work in the UK;
- Information from Disclosure and Barring Service (DBS) in order to administer relevant checks and procedures;

The Practice may collect this information in a variety of ways. For example, from application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you or through interviews

This personal data might be provided to us by you, or someone else (such as a former employer references, information from background check providers including criminal records checks permitted by law) or it could be created by us.

The Practice will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Your personal data will be stored in a range of different places, including in your application record, in the Practice's HR management systems and in other IT systems (including the Practice's email system).

Processing your personal data

The Practice will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- taking steps at your request prior to entering into a contract with you
- entering into a contract with you
- complying with any legal obligations
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We will process your personal data for the purposes of:

- assisting in decision making in recruitment and promotion procedures;
- assessing and confirming candidate's suitability for employment;
- maintaining accurate and up-to-date recruitment records;
- obtaining occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities and meet its obligations under health and safety law;
- ensuring effective general HR and business administration;
- obtaining references from third parties; and
- responding to and defending legal claims.

Special categories of personal data

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 job applicants with disabilities).

The Practice is obliged to seek information about criminal convictions and offences. Where we seek this information, we do so because it is necessary for us to carry out our obligations and exercise specific rights in relation to employment.

The Practice will not use your personal data for any purpose other than the recruitment exercise for which you have applied, however if your application is unsuccessful, the Practice may keep your personal data on file in case there are future job opportunities for which you may be considered. We will ask your consent to do this and you are free to withdraw your consent at any time.

Automated decision-making

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

Sharing your personal data

Your information may be shared internally for the purpose of the recruitment exercise, including with line managers or GP partners.

The Practice will not share your personal data with third parties, except those engaged for the purposes of the recruitment process, or 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, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal record checks.

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

Protection of personal data

The Practice has internal policies and controls in place to ensure that your personal data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the Practice engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Practical measures to ensure the security of data.

Retention of data

If your application is unsuccessful, the Practice will hold your personal data for a period of 6 months following the recruitment process. If you agree to allow the Practice to keep your personal data on file, for consideration for future job opportunities, we will hold your data for a further 6 months. At the end of that period (or once you withdraw consent), your data will be deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment.

Storing DBS Certificates

The correct storage of DBS certificate information is important. The code of practice requires that the information revealed is considered only for the purpose for which it was obtained and should be destroyed after six months.

<https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers#storing-information-for-dbs-certificate-information>

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this document.
- You have the right to access your own personal data by way of a subject access request
- You can correct any inaccuracies in your personal data.

- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- You have the right to be notified of a data security breach concerning your personal data
- With some exceptions, you have the right not to be subjected to automated decision making
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later.

If you would like to exercise any of these rights, or withdraw your consent, please contact the Practice Manager.

Accessing your data

We are legally required to act on requests and provide information free of charge with the exception of requests that are manifestly unfounded, excessive or repetitive.

If we determine this to be the case we may charge a reasonable fee or refuse to act on the request. We will acknowledge your request and provide the information within one month of receiving your request.

Please send your request to the Practice Manager.

Lodging a complaint

If you are not satisfied with our response or believe we are processing your personal information in a way that is not in accordance with the law, you have the right to lodge a complaint with the supervisory authority in the UK responsible for the implementation and enforcement data protection law: the ICO.

You can contact the ICO via the following:

Website: <https://ico.org.uk/concerns/>

Helpline: 0303 123 1113