Name of DPO: Michelle Wiles, Information Governance Manager

Contact address: Information Governance Team, Civic Centre, St Peters Square, Wolverhampton, WV1 1SH

Email: bcicbdpo@nhs.net

# **Darlaston Family Practice Privacy Notice**

**Introduction**

As part of any recruitment process, Darlaston Family Practice collects and processes personal information, or personal data, relating to job applicants. This personal information may be held by the Organisation on paper or in electronic format.

The DFP is committed to being transparent about how it handles your personal information, to protecting the privacy and security of your personal information and to meeting its data protection obligations under the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018. The purpose of this privacy notice is to make you aware of how and why we will collect and use your personal information during the recruitment process. We are required under the GDPR to notify you of the information contained in this privacy notice.

This privacy notice applies to all job applicants, whether they apply for a role directly or indirectly through an employment agency. It is non-contractual.

The Organisation has appointed a Data Controller to oversee compliance with this privacy notice. If you have any questions about this privacy notice or about how we handle your personal information, please contact the **Practice Manager** : Clinicalinfo.M91026@nhs.net

**How we use your information and the law**

We will only use your personal information when the law allows us to. These are known as the legal bases for processing. We will use your personal information in one or more of the following circumstances:

* where we need to do so to take steps at your request prior to entering into a contract with you, or to enter into a contract with you
* where we need to comply with a legal obligation
* where it is necessary for our legitimate interests (or those of a third party), and your interests or your fundamental rights and freedoms do not override our interests.

We need all the types of personal information listed under *“What types of personal information do we collect about you?”* primarily to enable us to take steps at your request to enter into a contract with you, or to enter into a contract with you, and to enable us to comply with our legal obligations. In some cases, we may also use your personal information where it is necessary to pursue our legitimate interests (or those of a third party), provided that your interests or your fundamental rights and freedoms do not override our interests. Our legitimate interests include: pursuing our business by employing employees, workers and contractors; managing the recruitment process; conducting due diligence on prospective staff and performing effective internal administration.

The purposes for which we are processing, or will process, your personal information are to:

* manage the recruitment process and assess your suitability for employment or engagement
* decide to whom to offer a job
* comply with statutory and/or regulatory requirements and obligations, e.g. checking your right to work in the UK
* comply with the duty to make reasonable adjustments for disabled job applicants and with other disability discrimination obligations
* ensure compliance with your statutory rights
* ensure effective HR, personnel management and business administration
* monitor equal opportunities
* enable us to establish, exercise or defend possible legal claims

Please note that we may process your personal information without your consent, in compliance with these rules, where this is required or permitted by law.

**What if you fail to provide personal information?**

If you fail to provide certain personal information when requested, we may not be able to process your job application properly or at all, we may not be able to enter into a contract with you, or we may be prevented from complying with our legal obligations. You may also be unable to exercise your statutory rights.

**Why and how do we use your sensitive personal information?**

We will only collect and use your sensitive personal information, which includes special categories of personal information and information about criminal convictions and offences, when the law allows us to.

Some special categories of personal information, i.e. information about your health, and information about criminal convictions and offences, is processed so that we can perform or exercise our obligations or rights under employment law and in line with our data protection policy.

We may also process information about your health and information about any criminal convictions and offences where we have your explicit written consent. In this case, we will first provide you with full details of the personal information we would like and the reason we need it, so that you can properly consider whether you wish to consent or not. It is entirely your choice whether to consent. Your consent can be withdrawn at any time.

The purposes for which we are processing, or will process, health information and information about any criminal convictions and offences, are to:

* assess your suitability for employment or engagement
* comply with statutory and/or regulatory requirements and obligations, e.g. carrying out criminal record checks
* comply with the duty to make reasonable adjustments for disabled job applicants and with other disability discrimination obligations
* ensure compliance with your statutory rights
* ascertain your fitness to work
* ensure effective HR, personnel management and business administration
* monitor equal opportunities

Where the Organisation processes other special categories of personal information, i.e. information about your racial or ethnic origin, religious or philosophical beliefs and sexual orientation, this is done only for the purpose of equal opportunities monitoring in recruitment and in line with our data protection policy. Personal information that the Organisation uses for these purposes is either anonymised or is collected with your explicit written consent, which can be withdrawn at any time. It is entirely your choice whether to provide such personal information.

We may also occasionally use your special categories of personal information, and information about any criminal convictions and offences, where it is needed for the establishment, exercise or defence of legal claims.

**Who has access to your personal information?**

Your personal information may be shared internally within the Organisation for the purposes of the recruitment exercise as well as our client who has the vacancy that you are applying for.

The Organisation will not share your personal information with third parties during the recruitment process.

If your job application is successful, our client will then take over the offer of employment or engagement. At that stage they will advise you who they may also share your personal information with including third parties (and their designated agents), including:

* external organisations for the purposes of conducting pre-employment reference and employment background checks
* the DBS, to obtain a criminal record check
* former employers, to obtain references
* professional advisors, such as lawyers
* outsourced provider such as payroll and HR

**How does the Organisation protect your personal information?**

The Organisation has put in place measures to protect the security of your personal information. It has internal policies, procedures and controls in place to try and prevent your personal information from being accidentally lost or destroyed, altered, disclosed or used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, workers, agents, contractors and other third parties who have a business need to know in order to perform their job duties and responsibilities. You can obtain further information about these measures from our Data Controller.

Where your personal information is shared with third parties, we require all third parties to take appropriate technical and organisational security measures to protect your personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law. We only allow them to process your personal information for specified purposes and in accordance with our written instructions and we do not allow them to use your personal information for their own purposes.

The Organisation also has in place procedures to deal with a suspected data security breach and we will notify the Information Commissioner’s Office (or any other applicable supervisory authority or regulator) and you of a suspected breach where we are legally required to do so.

**For how long does the Organisation keep your personal information?**

The Organisation will only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected and processed.

If your application for employment or engagement is unsuccessful, the Organisation will generally hold your personal information for six months, after the end of the relevant recruitment exercise but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal information for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. If you have consented to the Organisation keeping your personal information on file for in case there are future suitable employment opportunities, the Organisation will hold your personal information for a further six months after the end of the relevant recruitment exercise, or until you withdraw your consent if earlier.

If your application for employment or engagement is successful, personal information gathered during the recruitment process will be forwarded to our client who will then take over the offer of employment process.

Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IT systems and we will also require third parties to destroy or erase such personal information where applicable.

In some circumstances we may anonymise your personal information so that it no longer permits your identification. In this case, we may retain such information for a longer period

**Your rights over your personal information**

As a data subject, you have a number of statutory rights. Subject to certain conditions, and in certain circumstances, you have the right to:

* request access to your personal information - this is usually known as making a data subject access request and it enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
* request rectification of your personal information - this enables you to have any inaccurate or incomplete personal information we hold about you corrected
* request the erasure of your personal information - this enables you to ask us to delete or remove your personal information where there’s no compelling reason for its continued processing, e.g. it’s no longer necessary in relation to the purpose for which it was originally collected
* restrict the processing of your personal information - this enables you to ask us to suspend the processing of your personal information, e.g. if you contest its accuracy and so want us to verify its accuracy
* object to the processing of your personal information - this enables you to ask us to stop processing your personal information where we are relying on the legitimate interests of the business as our legal basis for processing and there is something relating to your particular situation which makes you decide to object to processing on this ground
* data portability - this gives you the right to request the transfer of your personal information to another party so that you can reuse it across different services for your own purposes.

If you wish to exercise any of these rights, please contact our Data Controller*.*We may need to request specific information from you in order to verify your identity and check your right to access the personal information or to exercise any of your other rights. This is a security measure to ensure that your personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you have provided your consent to the processing of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on your consent before its withdrawal. If you wish to withdraw your consent, please contact our Data Controller.  Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose you originally agreed to, unless we have another legal basis for processing.

If you believe that the Organisation has not complied with your data protection rights, you have the right to make a complaint to the Information Commissioner’s Office (ICO) at any time. The ICO is the UK supervisory authority for data protection issues.

**Objections/Complaints**

Should you have any concerns about how your information is managed or wish to object to any of the data collection at the Practice, please contact the Practice Manager or your healthcare professional to discuss how the disclosure of your personal information can be restricted. All patients have the right to change their minds and reverse a previous decision. Please contact the Practice if you change your mind regarding any previous choice.

If you would like to make a ‘data subject access request’ please contact the practice in writing. We will endeavour to respond to your request within one calendar month or two months if the request is complex.

Any changes to this notice will be published on our website and on the Practice notice board.

Suspected breaches in data protection can be reported to the Practice Data Protection Officer, Michelle Wiles at bcicbdpo@nhs.net. Breaches in data protection will result in an incident investigation. Serious breaches will be reported to the Information Commissioners Office (ICO).

It is the responsibility of all employees of the Practice to report suspected breaches of information security to the Practice Manager and Data Protection Officer without delay.

The Practice is registered as a data controller with the ICO. The registration number is Z609559X and can be viewed online in the [public register](https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/) or by contacting the ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything.  If you have any concerns about how your data is shared, then please contact the Practice Data Protection Officer, Caldicott Guardian or IG Lead.

If you would like to know more about your rights in respect of the personal data that we hold about you, please use the contact details below:

**IG Lead: Dr Shahid Merali**

**Caldicott Guardian: Dr Shahid Merali**

**Data Protection Officer: Michelle Wiles, Information Governance Manager – Black Country**