Data Protection Privacy Notice for Candidates Applying for Work

Introduction

For the purpose of applicable data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the GP practice responsible for your personal data is **Charnwood Surgery**.

We, Charnwood Surgery, are the **Controller** of the personal data you provide to us. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This Privacy Notice applies to personal information processed by or on behalf of the Practice. It applies to the personal data of individuals applying for work at Charnwood Surgery and to data collected during recruitment which may later form part of an employee personnel file.

Contents

- Why do we need your data?
- What data do we collect about you?
- What is the legal basis for using your data?
- How do we store your data?
- Our systems and data processors
- How do we maintain the confidentiality of your data?
- How long do we keep your data?
- What are your data protection rights?
- Who do we share your data with?
- When is your consent not required?
- What should you do if your personal information changes?
- Changes to our privacy policy
- Our Data Protection Officer
- How to contact the appropriate authorities

Why do we need your data?

We need to know your personal, sensitive and confidential data in order to manage recruitment, assess your suitability for roles, fulfil employment and safeguarding obligations, and, where applicable, enter into and perform an employment contract with you.

Information may also be used within the Practice for recruitment audit and to monitor the quality and fairness of our recruitment processes.

What data do we collect about you?

Personal data

When you apply for a role at Charnwood Surgery, we will ask you to provide personal information including:

- Name
- Address
- Telephone numbers
- Email address
- Date of birth
- Previous employment data

- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies
- Details of your employment history, skills and experience
- Information about your current level of remuneration, including benefit entitlements
- Information in relation to your right to work in the UK (for example documents and checks in line with "Prove your right to work to an employer" and the Home Office Right to Work Checklist)

We may collect this information from application forms, CVs, online applications, identity documents (such as passports and driving licences) and from interviews, meetings or assessments (including online tests).

Special category personal data and criminal records
We may also process the following special category or sensitive information:

- Health or medical information where required to make reasonable adjustments during the recruitment process or to meet occupational health requirements
- Vaccination and immunisation status where required for healthcare roles and infection prevention and control
- Information about criminal convictions and offences (for example via Disclosure and Barring Service (DBS) checks) where required for safeguarding and legal/regulatory purposes
- Information about ethnic origin, sexual orientation, religion or belief, collected for equal opportunities monitoring in line with employment law (normally analysed in an anonymised or aggregated form)

This personal data is usually collected directly from you as part of your application. However, we may also obtain information about you from third parties where relevant to the recruitment process. These may include recruitment agencies, former employers (for references), background check providers, occupational health providers, and NHS bodies involved in employment verification. We only collect information from these sources where it is necessary, lawful and proportionate for recruitment, safeguarding and employment purposes.

What is the legal basis for using your data?
We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- NHS Codes of Confidentiality, Information Security and Records Management

Under the UK GDPR, we rely on the following legal bases for processing candidate data:

- **Article 6(1)(b)** – processing is necessary for the performance of, or to take steps at your request prior to entering into, an employment contract (for example assessing your application and issuing an offer of employment)

- **Article 6(1)(c)** – processing is necessary for compliance with a legal obligation (for example right to work checks, safeguarding and NHS employer requirements)
- **Article 6(1)(f)** – processing is necessary for our legitimate interests in managing and improving our recruitment processes, ensuring fairness and consistency in selection, assessing candidate suitability, preventing fraud, and maintaining the safety and integrity of our services. We have carried out a legitimate interests assessment to ensure that our interests do not override your rights and freedoms. You have the right to object to this processing where applicable.
- **Article 6(1)(a)** – your explicit consent where we ask for it (for example to keep your details on file for future vacancies)

For special category data we rely on:

- **Article 9(2)(b)** – processing is necessary for carrying out obligations and exercising specific rights in the field of employment and social security law (for example disability and occupational health information)
- **Article 9(2)(h)** – processing is necessary for the purposes of occupational medicine and the assessment of your working capacity (for example occupational health assessments and vaccination status)
- **Article 9(2)(g) / 9(2)(i)** – processing is necessary for reasons of substantial public interest, including safeguarding and regulatory requirements in healthcare where applicable

Where we process information about criminal convictions and offences (for example, Disclosure and Barring Service checks), this is carried out in accordance with Article 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018. This processing is necessary for employment, safeguarding and regulatory requirements in healthcare and is carried out under appropriate safeguards including restricted access, secure storage, and retention in line with DBS Code of Practice.

We do not make recruitment decisions based solely on automated processing. All decisions involve human review.

How do we store your data?

We have a data protection regime in place to oversee the effective and secure processing of your personal and special category data.

All personal data we process is handled by our Practice within the UK; for IT hosting and maintenance, information may be stored on secure servers within the UK or European Union, or within NHS-approved secure cloud services, with appropriate safeguards and contracts in place.

Your personal data will be stored in a range of places including:

- Your application record and recruitment files
- HR management systems
- Secure network drives and email systems
- Occupational health records (where applicable)

No third parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place.

Our systems and data processors

To manage recruitment safely and efficiently we may work with trusted systems and data processors under strict data processing agreements. These organisations process your data only on our instructions and must keep it secure and confidential.

Examples include (where used by the Practice):

- HR and payroll systems used to create and maintain personnel records for successful candidates
- NHS employment verification systems (for example NHS Digital or other NHS bodies)
- Occupational health providers engaged to carry out pre-employment health assessments
- Secure email and electronic document management systems used to store recruitment documentation

All processors are required to:

- Process data only under our written instructions
- Maintain appropriate technical and organisational security measures
- Ensure staff confidentiality obligations
- Assist with data subject rights requests
- Delete or return data when services end

How do we maintain the confidentiality of your data?

Our Practice policy is to respect the privacy of candidates, staff and patients and to maintain compliance with the UK GDPR and all UK-specific data protection requirements.

We use a combination of working practices and technology to ensure that your information is kept confidential and secure. Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

All employees and sub-contractors engaged by the Practice are asked to sign a confidentiality agreement. Where a sub-contractor acts as a data processor (for example for archiving or HR systems), an appropriate Data Processing Agreement is established for the secure processing of your information.

We only share your information with those who have a genuine need and where the law allows.

How long do we keep your data?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records Management Code of Practice for Health and Social Care and in accordance with National Archives requirements.

If your application is unsuccessful, we will normally hold your personal data for six months following the recruitment process. If you agree that we may retain your details for

consideration for future job opportunities, we will keep your data for a further six months, after which it will be securely deleted or destroyed unless you renew your consent.

If your application is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained for the duration of your employment and for any additional period required by law and NHS records retention schedules.

DBS certificate information is kept securely, used only for the purpose for which it was obtained and normally destroyed after six months, in line with DBS Code of Practice guidance.

More information on records retention can be found at NHSE – Records Management Code of Practice.

What are your data protection rights?

Even if we already hold your personal data, you have certain rights in relation to it. These include:

- Right of access – You have the right to request a copy of the personal data we hold about you.
- Right to rectification – You have the right to request correction of inaccurate or incomplete personal data.
- Right to erasure – In certain circumstances, you have the right to request that we delete your personal data.
- Right to restrict processing – You have the right to request that we limit the way we use your personal data in certain circumstances.
- Right to data portability – You may request that we transfer your data to another organisation, or to you, where technically feasible.
- Right to object – You can object to processing based on our legitimate interests; we will consider your request in line with legal requirements.
- Right to withdraw consent – Where we rely on your consent, you may withdraw it at any time.
- Right to lodge a complaint – You have the right to lodge a complaint with the UK supervisory authority, the Information Commissioner's Office.

To exercise any of these rights, please contact the Practice Manager or our Data Protection Officer (details below). We may ask for proof of identity before fulfilling your request. Requests should ideally be made in writing. We aim to respond within one month, as required by data protection law.

Who do we share your data with?

Your information may be shared internally for the purposes of the recruitment exercise, including with:

- Members of the HR and recruitment team
- Interviewers involved in the selection process
- Managers in the department with the vacancy
- IT staff where access to the data is necessary for the performance of their roles
- Occupational health services (if required)

We will not share your personal data with third parties except:

- Where they are engaged for the purposes of the recruitment process (for example recruitment agencies, occupational health providers, background check providers)
- Where your application is successful and we make you an offer of employment (for example former employers for references, the Disclosure and Barring Service for criminal record checks, NHS Digital or other NHS bodies for employment verification)
- Where we are legally required to do so or where it is necessary for safeguarding or regulatory reasons in healthcare settings.

We do not routinely transfer your data outside the UK. Where this is necessary, we ensure appropriate safeguards are in place, such as adequacy regulations or Standard Contractual Clauses.

In most cases, we rely on lawful bases other than consent to process your data (for example, performance of a contract, legal obligations, or legitimate interests).

Where we do rely on your consent—for example, to retain your details for future job opportunities—we will ask for it explicitly. You have the right to withdraw consent at any time.

Consent is not required for other lawful processing necessary for recruitment, safeguarding, regulatory compliance, or employment obligations.

We do not use your recruitment information for marketing purposes and we do not routinely review candidates' personal social media profiles as part of our vetting.

When is your consent not required?

We will only ever use or pass on information about you to others if they have a genuine need for it and it is lawful to do so.

There are circumstances where we are required by law to disclose information without your consent, for example:

- Where there is a serious risk of harm or abuse to you or other people
- Where a serious crime is being investigated or could be prevented
- Where a formal court order has been issued
- Where there is another specific legal requirement to share information (for example safeguarding or regulatory investigations)

We also act in accordance with the Caldicott Principles, including the principle that the duty to share information can be as important as the duty to protect confidentiality when it is in the public interest or necessary to protect individuals from harm.

What should you do if your personal information changes?

Please tell us if your personal details change so that we can keep our records accurate and up to date.

You should contact the Practice Manager as soon as possible to update details such as your address, telephone number or email address.

Changes to our privacy policy
We may amend this Privacy Notice from time to time. Any changes will be published on our website and, where appropriate, notified to you by email or during the recruitment process.

This notice was last updated in March 2026. We review it annually or when significant changes occur.

Our Data Protection Officer
The Practice has appointed **Umar Sabat** as its Data Protection Officer.

He can be contacted by email at **umar.sabat@ig-health.co.uk** or by calling **07894 826 037**.

If you have any concerns about how your data is used or about your rights in respect of your personal data, please contact the Data Protection Officer in the first instance.

How to contact the appropriate authorities
If you have any concerns about how your information is managed at Charnwood Surgery, please contact the **Practice Manager** or the **Data Protection Officer** first.

If you are still unhappy following a review by the Practice, you have the right to lodge a complaint with the UK supervisory authority, the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk/