

UK BIOBANK PRIVACY NOTICE FOR CANDIDATES

UK Biobank respects your privacy and is committed to protecting the privacy and security of your personal data.

UK Biobank is a "controller" in relation to personal data. This means that we are responsible for deciding how we hold and use personal information about you.

You have received a copy of or been provided with a link to this privacy notice because you are applying or are considering applying to work with us, or adding yourself to our talent pool to be considered for future vacancies (whether as an employee, worker or contractor). It explains how we collect, share and use personal information about you for the purposes of the recruitment exercise, and how long it will usually be retained for in accordance with the UK General Data Protection Regulation (UK GDPR).

The personal data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

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

- **(a) Identity Data** – includes your name, title, gender/sex, date of birth and other information contained in identity documents (such as passports, visa, work permits, birth certificate).
- **(b) Contact Data** – includes your postal address, email address and telephone numbers.
- **(c) Recruitment Data** – includes any information provided to us in your CV, covering letter, application, right to work documentation and from your references. This also includes your employment history, qualifications, any information you provide to us during an interview, undertaking a test or delivering a presentation.

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

- **(d) Equal Opportunities Data** – includes information about your race, nationality or ethnicity, religious beliefs, sexual orientation.
- **(e) Medical/Health Related Data** – includes information about your health, including any medical condition, health and sickness records.
- **(f) Criminal Convictions Data** – includes information about criminal convictions and offences.

How is your personal data collected?

We collect personal data about candidates through the application and recruitment process from the following sources:

- **Direct interactions with you** – you may give us your Identity Data, Contact Data, Recruitment Data, Equal Opportunities Data, Medical/Health Related Data and Criminal Convictions Data by corresponding with us by post, phone, email or other online methods.
- **Recruitment agencies** – we may collect Identity Data, Contact Data and Recruitment Data from recruitment agencies by post, phone, email or other online methods.
- **Applicant Tracking System** – we use an online software product provided by The Infuse Group Ltd (t/a Pinpoint Software) to assist with our recruitment process and we may collect collect Identity Data, Contact Data, Recruitment Data and Equal Opportunities Data using this system.
- **Disclosure and Barring Service** – we may receive Identity Data and Criminal Convictions Data from the Disclose and Barring Service (DBS) by email, if applicable for the role.
- **References** – we may receive Recruitment Data from your named references and former employers, which may include the following categories of data: Confirmation of:
 - period of employment (start/leaving dates);
 - confirmation of job title and indication of ability to perform job being offered;
 - any current disciplinary action; and
 - how long the referee has known the applicant and in what capacity.
- **Occupational health provider/professionals** – we may receive Medical/Health Related Data from our occupational health provider/professionals by email or other online methods when we use an external provider to manage the medical questionnaire on our behalf.

How we use personal data about you

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.
- Where it is necessary for reasons of substantial public interest.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
Communicating with you about the recruitment process	(a) Identity Data (b) Contact Data	Necessary for our legitimate interests – we want to communicate with you in order to run the recruitment process
Assessing your skills, qualifications and suitability for the role	(a) Identity Data (c) Recruitment Data	Necessary for our legitimate interests – we want to ensure the candidate is suitably skilled and qualified to perform the role applied for
Checking you are legally entitled to work for us	(a) Identity Data (b) Contact Data (c) Recruitment Data	Necessary to comply with a legal obligation
Carrying out background and reference checks, where applicable	(a) Identity Data (b) Contact Data (c) Recruitment Data (f) Criminal Convictions Data	Necessary for our legitimate interests – we want to ensure the candidate is suitable for the role applied for
Equal opportunities monitoring	(d) Equal Opportunities Data	Necessary for reasons of substantial public interest - for the purposes of equal opportunity monitoring and reporting
Considering if any appropriate adjustments need to be made to the recruitment process	(e) Medical/Health Related Information	Necessary for reasons of substantial public interest – to comply with the Equality Act 2010, for example making adjustments during the recruitment process for any test or interview
Keeping records relating to our hiring processes	(a) Identity Data (b) Contact Data (c) Recruitment Data	Necessary to comply with a legal obligation Necessary for our legitimate interests – to defend any legal claims
Making a decision about your recruitment or	(c) Recruitment Data (f) Criminal	Necessary to comply with a legal obligation: - We are legally required by the

<p>appointment, including taking into account the nature of the criminal conviction (only where it has an impact on the ability to carry out a role or breaches a legal requirement)</p>	<p>Convictions Data</p>	<p>Health & Care Professionals Council to carry out criminal record checks for those carrying out a role within our Imaging Clinics.</p> <ul style="list-style-type: none"> - The role of Radiographer and Health Care Assistants/Team Leaders are roles which are listed in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023) and the Police Act 1997 (Criminal Records) Regulations (SI 2002/233). These roles are therefore eligible for enhanced checks from the Disclosure and Barring Service.
--	-------------------------	---

If you fail to provide personal data

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, if we require a criminal record check, or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

Automated decision-making

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

Data sharing

Why might you share my personal data with third parties?

We will only share your personal data with the following third parties for the purposes of processing your application:

- Stockport Council for processing a DBS application (where applicable); and
- Occupational health professionals in respect of information in your medical questionnaire completed by you at job offer stage.
- Applicant Tracking System we use an online software product provided by The Infuse Group Ltd (t/a Pinpoint Software) to assist with our recruitment process

All our third-party service providers and other third parties are required to take appropriate security measures to protect your personal data 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.

Data security

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

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.

Data retention

How long will you use my data for?

We will retain your personal data for a period of 12 months from either (i) the time you apply for a job, or (ii) the time you add your CV to our talent pool. If you interact with us again during that 12 month period (or any extension of it) we will extend the retention period by 3 months from the date of that interaction. . After this period (if you have been unsuccessful), we will securely destroy your personal data in accordance with our data retention policy.

Your data protection rights

Under certain circumstances, you have rights under data protection law in relation to your personal data. These legal rights are briefly summarised below, in relation to any personal data about you which we hold.

- **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 lawfully processing it.
- **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).
- **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. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **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.

If you want to exercise any of these rights please either:

- Where your data has been added to the applicant tracking system provided by The Infuse Group Ltd (t/a Pinpoint Software) you can utilise the 'Manage your Data' tool provided within that system: or
- Contact our data protection officer either by email dpo@ukbiobank.ac.uk or via post: The Data Protection Officer, UK Biobank, Units 1-2 Spectrum Way, Adswood, Stockport, SK3 0SA. ,

Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal data, please contact the DPO at dpo@ukbiobank.ac.uk or via post: The Data Protection Officer, UK Biobank, Units 1-2 Spectrum Way, Adswood, Stockport, SK3 0SA. . 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.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

.