General Data Protection Regulations 2018
Recruitment & Selection

Privacy Statement:
At Nouvita Healthcare, we take your privacy seriously and will only use your personal information to administer your application for employment. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and if you would like more information on a particular topic, please contact our Data Protection Officer, Harriet Anstey on 01707 932120.

Personal Data We Collect
We collect the following personal data relating to your employment application:

- Contact Details (Name, Address, Email Address, Telephone &/or Mobile Number)
- Employment history
- Qualifications
- Equality of Opportunity (Ethnicity, Disability Details) under Special Categories

Special category personal data
We may need to process special category personal data to ensure a fair recruitment process. If a candidate informs us that any adjustments are needed (e.g., wheelchair user or visually impaired) we will be sure to document this and keep it safe and secure, and made available to those who need access to this data. This data will also be held for as long as necessary as part of our data retention guidelines.

How We Use Personal Data
Your personal data will be used to process your employment application.

How Long We Will Hold Personal Data
We retain recruitment data for as long as needed as part of our recruitment process. If you have not been successful, we will typically retain this data for a period of 6 months so we can show and evidence a fair recruitment process and there is no discrimination on any protected characteristics/grounds. After this period has ended all relevant data will be securely destroyed. Successful candidates will have their recruitment data added to their HR file which is maintained and held by our head office for up to six years after employment ceases.

Data Sharing
Personal data of job applicants can be shared between different functions HR functions within our head office. We do this to ensure the recruitment process has been carried out in accordance with our recruitment policies and the appropriate files can be created and maintained. We do not share personal data with any third parties, but may do so where:

- There is an issue that puts the safety of our staff at risk
- We need to liaise with other agencies or third parties – we will seek consent as necessary before doing this

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
  In connection with legal proceedings
- Where the disclosure is required to satisfy our legal obligations

How We Protect Your Personal Data
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.

If we become aware of any loss, misuse, alteration of personal data we will work closely with our IT team, DPO and other parties as necessary to investigate the incident at hand. We have put into place the relevant procedure and policies in place to investigate, mitigate and report (when needed to relevant parties) such instances.

How to Access & Control Your Personal Data
Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

<u>Subject access requests can be submitted verbally or in writing to the DPO, detailing:</u>

- Your name
- Your correspondence address
- Your contact number and email address
- Full details of the information being requested

When responding to requests, we:

- May ask the individual to provide 2 forms of identification irm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual: In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)