AJ Case Management Ltd - Recruitment Privacy Statement
(V003 22.02.19)

Background

A J Case Management Ltd offers and provides bespoke Clinical services to our clients across the England and Wales. As part of our offering we recruit staff on behalf of our clients or their Deputies as the Employer. This privacy policy covers how we protect the data that is supplied to us by our clients, job applicants and agencies.

Our Commitment to Job applicants

AJ Case Management Ltd believes completely in equal opportunities and will treat all applicants fairly with no discrimination.

We never knowingly provide misleading information about the nature of the role.

AJ Case Management Ltd is committed to managing your personal information securely and with respect and in accordance with the General Data Protection requirements.

This Privacy Policy outlines how we collect, use, store and disclose the information about you that we hold.

The information we collect may cover the following:

- Contact information (name address, phone number and email address)
- Information from CV or application form (education, skills and qualifications)
- Psychometric tests (e.g. Via Institute on Character, Thomas International DISC profile)
- Health records (Health questionnaires) where required as part of the role.
- Occupational health report (Higher level screening required for role) with Access to medical Records consent being given by the applicant
- Disclosure and Barring Record where a requirement for the role
- References from the named referees that the applicant provides and only with the applicant's consent
- Visa and proof of the right to work in the UK documents
- Employment records (including job titles, work history, working hours, training records and any professional memberships
- Payroll Information (Bank details, P45, P46) –
- Next of Kin and Emergency contact details
- Driving licence and licence summary via DVLA portal

Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within our client's support teams, and checking you are legally entitled to legally work in the UK.

Your information will be passed to the Associate Case Manager and sometimes the client or their representatives to be considered for the vacancy. We collect personal information directly from candidates. Where appropriate, we will collect information about criminal convictions as part of the recruitment process. We are allowed to use your personal information in this way to carry out our obligations necessary for the performance of the contract.

How the information is held.

Information is transmitted by email and is stored on our computers, our electronic file storage system and/or paper-based filing.

All this information can only be accessed by authorised AJ Case Management Ltd staff or the Associate Case Manager. Our staff are trained to understand the importance of keeping personal data secure.

Our computers are safeguarded by anti-virus software and the regular changing of security passwords

The information on candidates will be held for 6 months in line with CIPD recommended best practice. (Where preferred by the Employer, AJ Case Management will hold the documents securely for the duration of the contract of service). After which any paper based or electronic recruitment files for successful candidates will be securely transferred to the Employer or the Employers Deputy. On our confirmation of safe receipt all paper-based records will be securely shredded, and electronic records held by AJ Case Management will be deleted. At this time files for unsuccessful candidate's information will be securely deleted. Only if you have given your written consent for the data to be held will this not apply.

Disclosure

We may disclose the information for the purpose it was collected to our Clients or their representatives, Associate Case Managers, client's legal teams and referees. Where additional information is required the information may be disclosed to the Disclosure and Barring Service, your G.P or an Occupational Health professional only after you have given your consent.

You have specific rights in connection with personal information: request access to your personal information; **request correction** of the personal information that we hold about you; **request erasure** of your personal information; **object to processing** of your personal information where we are relying on a legitimate interest; **request the restriction of processing** of your personal information; **request the transfer** of your personal information to another party and the **right to withdraw consent.**

Complaints

Privacy complaints are taken very seriously and if you believe that we have breached your privacy you should in the first instance write to our Privacy Officer Sharon Richards-Glover the details of your complaint. We would ask that you provide us with as much detail as possible to allow a thorough investigation. Your complaint will be acknowledged within 24 hours and we aim to resolve any complaint within 5 working days. However, depending on the complexity of the complaint and availability of clients or external agencies it may on occasions take longer.

Should your complaint show that we have breached our duty of care we will report the breach to the ICO.

If you are not satisfied by our response you may complain to the ICO.