Recruitment

Privacy and Data retention policy

May 2018
Reviewed November 2018
Reviewed November 2020

SEQOHS
Safe Effective Quality Occupational Health Service

ISO 9001 2015 FS 557227

Commitment to social enterprise

Bringing health to life

1. Introduction

This privacy policy covers how we collect, use, store and protect the data that is supplied to us by job applicants and agencies.

Our Commitment to Job applicants

We believe 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.

We are committed to managing your personal information securely and with respect in accordance with the General Data Protection Requirements.

The information we collect may cover the following:

- Contact information (name address, phone number and email address)
- Information from CV or application form or covering letter (education, skills and qualifications)
- Health records (night worker assessment forms, health questionnaires) where required as part of the role.
- Disclosure and Barring Record where a requirement for the role
- References from 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 professional memberships)
- Salary, annual leave, pension and benefits information.
- Driving license, motor insurance, MOT [if applicable]

We may also collect, store and use 'special categories' of more sensitive personal data which require a higher level of protection such as information about your race or ethnicity, religious beliefs, sexual orientation and political opinions. Also information about criminal convictions and offences.

Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within our organisation and checking you are legally entitled to work in the UK. Your information will be used in consideration for the vacancy currently available or, with your consent, for potential future vacancies that might arise.

How the information is collected

We collect personal information through the application and recruitment process, either directly from candidates, or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers or other background check agencies including the NMC, GMC or other professional bodies and insurers. We may collect additional personal information in the course of job-related activities should your application be successful.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process. We will only do this if it is appropriate given the nature of your role and where we are legally able to do so. We envisage that we will access your DBS portal.

How the information is held

Most information is transmitted by email and is stored on our computers and paper based filing. We use Microsoft Sharepoint which covers our email servers and cloud based file storage system.

All this information can only be accessed by authorised personnel. 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 for specific roles will be held for six months in line with CIPD recommended best practice. After which, paper files will be securely shredded and computer records deleted. Only if we have asked, and you have given your consent for the data to be held, will this not apply.

Your rights

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 data protection officer, Helen Hooper, stating 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 five 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 Information Commissioner's Office.

If you are not satisfied by our response you may complain to the Information Commissioner's Office (ICO): www.ico.org.uk

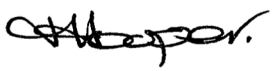
Contact details

MOHS Workplace Health: Helen Hooper, data protection officer, helenhooper@mohs.co.uk / 0121 601 4041

Changes to this privacy and data retention notice

We reserve the right to update this privacy notice at any time for justifiable reasons.

For further information, please refer to our Data Protection Policy.

Signed		Name	Helen Hooper
Title	Chief Executive	Date	November 2020