

## Recruitment Privacy Statement

### Background

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

### Our Commitment to Job applicants

Colchester and Tendring Women's Refuge 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. We would never charge a job seeker a fee for the purpose of finding them a role.

Colchester and Tendring Women's Refuge 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)
- Health records 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

### Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within our client's organisations.

### How the information is held

Information is transmitted by email and is stored on our computers and / or paper-based filing.

The paper based filing can only be accessed by authorised staff. 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 unsuccessful candidates will be held for 6 months in line with CIPD recommended best practice. After which paper files will be securely shredded and computer records deleted. Only if you have given your consent for the data to be held will this not apply.

### **Disclosure**

We may disclose the information for the purpose it was collected to clients and referees. Where additional information is required the information may be disclosed to the Disclosure and Barring Service, your Doctor or an Occupational Health professional.

### **Access and Corrections**

Under the GDPR you have the right to access and seek correction of your personal information. This may be to add an additional qualification you have gained or a change of address. We will ask for proof of ID before allowing access and proof of additional qualifications. We will then ensure that the information we hold is updated. We do ask you to allow us time to make the changes which we will complete within 5 working days.

### **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 the Eleanor Burgoyne 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 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.