

Privacy Notice for Job Applicants

Privacy statement for job applicants

Islington Mind is a data controller and we collect and process personal data relating to job applicants as part of any recruitment process. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

What information do we collect?

We collect and process a range of information about you. This includes

- Your name, address and contact details, including email address and telephone number;
- Details of your qualifications, skills, experience and employment history;
- Information about your current level of remuneration, including benefit entitlements;
- Whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- Information about your entitlement to work in the UK; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief. This information is anonymised before processing.
- If you attend an interview, your image on our CCTV systems in/out of the office, properties or communal areas which is covered at that facility
- We may use video conferencing for meetings and interviews (such as MS Teams). After you join a meeting, we may **start recording and transcription**. A notification appears so everyone in the meeting knows that the recording has started. You must notify a member of staff if you do not wish for the interview to be recorded.

We collect this information in a variety of ways. For example, data might be contained in application forms, CVs obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

We will also collect personal data about you from third parties, such as references supplied by former employers and information from criminal records checks. We will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why do we process personal data?

We need to process data to take steps at your request prior to entering into a contract with you. We also need to process your data to enter into a contract with you.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims. Where we rely on legitimate interests as a reason for processing data, we have considered whether or not those interests are overridden by the rights and freedoms of employees or workers and have concluded that they are not.

We process health information if we need to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

Where we process other special categories of data, such as information about ethnic origin, sexual orientation, health, religion or belief, age, gender or marital status, this is done for the purposes of equal opportunities monitoring with the explicit consent of job applicants, which can be withdrawn at any time.

For some roles, we are obliged to seek information about criminal convictions and offences. Where we seek this information, we do so because it is necessary for us to carry out our obligations and exercise specific rights in relation to employment.

We will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to your data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the People & Culture and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

We use a third party to collect and process job applications on our behalf however we will not share your data with any other third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

We will not transfer your data to countries outside the European Economic Area (EEA) and where data may be transferred outside of the EEA by third parties we will seek assurances that this is done in line with data protection legislation.

How do we protect your data?

We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

How long do we the keep your data?

If you are unsuccessful after being interviewed the organisation will hold your data on file for 6 months after the end of the relevant recruitment process.

CCTV recordings are not held longer than 30 days.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. Details about the periods for which your data will be held are included in our employee privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require us to change incorrect or incomplete data;
- Require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where we are relying on legitimate interests as the legal ground for processing; and
- Ask us to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing data.

If you would like to exercise any of these rights, please

contact admin@islingtonmind.org.uk

If you believe that we have not complied with your data protection rights, you have the right to complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Automated decision-making

We do not make any decisions based solely on automated decision-making during our recruitment processes.

Who can I contact if I have any questions?

For further information you can contact Christian Action's Data Protection Officer as follows:

The Data Protection Officer

Archway Business Centre

Unit 4

Wedmore Street

N19 4RU

E-mail: admin@islingtonmind.org.uk

You can find more information about your rights around how we handle your personal data from the Information Commissioners Office on **0303 123 1113** or via their website www.ico.org.uk