

Privacy Policy

Recruit with Purpose Limited

Version 2.0 | Updated 21 October 2026 | Review due 21 October 2027

1 Who we are and how to contact us

Recruit with Purpose Limited (RWP, we or us) is the controller of the personal information described in this notice. We provide permanent, interim and contract recruitment services, specialising in social housing. We handle personal information under the UK GDPR, the Data Protection Act 2018 and applicable Privacy and Electronic Communications Regulations, as amended, including by the Data (Use and Access) Act 2025.

Registered office: 27 Mortimer Street, London, United Kingdom, W1T 3BL.

Privacy enquiries and requests: contact@recruitwithpurpose.co.uk

Privacy lead: Henry Ivall, Director — henry@recruitwithpurpose.co.uk

This notice covers prospective and placed candidates, agency workers and contractors, client and supplier contacts, referees, website visitors, and people attending our events or participating in our professional communities. It also covers applications to work for RWP. If we employ you directly, we will provide additional privacy information about employment administration.

2 Where we obtain information

We collect information directly when you apply for a role, send a CV, complete a website form, speak or correspond with us, provide services, register for an event or participate in a community such as SHIIIFT.

We may also obtain relevant information from LinkedIn and other public professional profiles, employer websites, industry directories, job boards and CV databases such as Totaljobs, CV-Library and Reed; from clients, referees and people making referrals; and from authorised identity, right-to-work or background-checking services where appropriate.

If we obtain your information indirectly, we will tell you the source and provide this notice within a reasonable period, normally no later than one month, or at our first communication or first disclosure if earlier, unless a lawful exception applies.

3 Information we collect

We collect information relevant to the purpose and stage of our relationship, rather than every category about every person. The main categories are described on the next page. Please avoid sending sensitive or unrelated personal details unless they are needed for a specific purpose we have explained.

3 Information we collect continued

Candidates and workers: name, contact details, location, CV, work history, qualifications, professional registrations, skills, availability, job preferences, remuneration expectations, applications, interview feedback, references and relevant correspondence. Where needed, we also collect identity, date of birth, nationality and right-to-work evidence; assignment terms, working time, bank, tax and National Insurance details; and details of any company or umbrella arrangement through which you work.

Business contacts and referees: name, employer, role, business contact details, relationship history, correspondence, references and information needed for contracts, invoicing and supplier administration.

Website and event users: enquiries, registration details, attendance, preferences, feedback and relevant technical information such as IP address, browser/device details and website interactions. Sections 5 and 11 explain sensitive information, recordings and cookies.

4 Why we use information and our lawful bases

Purpose	Lawful basis and explanation
Recruitment and candidate relationships	Legitimate interests in identifying suitable people, matching skills to vacancies, maintaining relevant candidate relationships and providing recruitment services. Contract applies where processing is necessary for a contract directly with you or steps you ask us to take before it.
Worker engagements and payments	Contract for administering your direct engagement and paying you; legal obligation for applicable employment, tax, payroll and right-to-work duties. Legitimate interests for necessary coordination with a client or umbrella company where our contract is with them.
Client and supplier relationships	Legitimate interests in providing and obtaining services, managing contacts, invoicing and credit control. Contract applies if you personally are a party; legal obligation applies to required accounting and tax records.
Events and professional communities	Legitimate interests in organising requested participation, sharing relevant professional information and improving events. Consent is used where required for optional activities or electronic marketing; see section 11.
Marketing and service improvement	Legitimate interests in relevant business development, feedback and improving our services, subject to your rights. Consent where electronic-marketing or tracking rules require it; see section 11.
Security, compliance and disputes	Legal obligation for required records and disclosures. Legitimate interests in protecting systems, preventing fraud, resolving complaints and establishing, exercising or defending legal claims.

When relying on legitimate interests, we assess necessity and balance our interests against your rights and reasonable expectations. Publicly available information is still personal information. You may object as explained in section 13.

5 Sensitive information and criminal records

Health or disability information and racial or ethnic origin are special category data. We only request these where necessary for an explained purpose, such as reasonable adjustments, employment duties or optional equality monitoring. An ordinary lawful basis is not enough: a separate legal condition is also required.

For health information necessary to fulfil employment-law or social-protection duties, we rely on legal obligation, the employment condition in Article 9(2)(b) of the UK GDPR and Schedule 1 paragraph 1 of the Data Protection Act 2018. For optional equality monitoring or other voluntary sensitive information, we seek explicit consent where appropriate, covering both the ordinary basis and special category condition. For necessary legal claims, legitimate interests and the Article 9(2)(f) legal-claims condition may apply. We explain the relevant purpose and condition when requesting information and apply any required additional safeguards.

Criminal convictions, offences and related allegations are subject to separate rules under Article 10; they are not special category data. We only undertake checks where justified for the role, at a legally permitted level, with an ordinary lawful basis and an applicable Schedule 1 condition. We will explain the particular check, legal condition and recipients before it takes place. A client request or general consent does not, by itself, authorise every type of check.

6 Whether you must provide information

You can choose whether to use our services or provide optional information. Some information is necessary to assess an application, meet a legal requirement or administer a contract. For example, without relevant identity or right-to-work evidence we may be unable to progress an engagement; without payment details we may be unable to arrange payment. We will explain any requirement and the consequences when asking. Optional equality-monitoring or marketing choices do not determine whether we provide recruitment services.

7 Who we share information with

- Clients and their recruitment partners: relevant application information, interview arrangements and placement details, including with managed service or recruitment-process providers. We discuss the opportunity with you and obtain your agreement before submitting an identifiable CV to a client.
- Engagement and verification providers: umbrella/payroll companies, referees, identity and right-to-work providers, and lawful background-checking services where needed. If you ask for a referral to an insurer or other provider, we share only the necessary details.
- Business service providers: recruitment database/CRM, hosting, cloud storage, email, telephony, event, survey, analytics and IT support providers, and professional advisers such as accountants, lawyers and insurers, where necessary for their services.
- Authorities and other necessary recipients: HMRC, regulators, law enforcement or courts where legally required or otherwise lawful, and relevant parties where necessary for legal claims or a business transfer, subject to appropriate safeguards.

Providers processing information for us must act under appropriate contractual instructions and confidentiality/security obligations. Clients, umbrella companies and some other recipients may act as independent controllers and provide their own privacy notices. We share only relevant information. Limited client-contact details may be provided to candidates to arrange interviews or an assignment.

8 International transfers

We operate in the UK, but some service providers may store or access personal information outside the UK. Overseas remote access can also amount to an international transfer. The protections we use depend on the provider, destination and arrangement.

Where a transfer is restricted under UK data protection law, we use UK adequacy regulations where applicable, or an appropriate safeguard such as the UK International Data Transfer Agreement or the UK Addendum to the European Commission's standard contractual clauses. Where required, we assess the protection available, carry out the applicable data protection test and put additional measures in place. Any exceptional transfer must satisfy a specific legal exception; routine transfers are not justified simply by a general consent clause.

You can contact our privacy lead for information about the destinations and safeguards relevant to your information and a copy of the applicable safeguards, subject to necessary redactions to protect confidential information.

9 Keeping information secure

We use appropriate organisational and technical measures to protect personal information from unauthorised access, loss, misuse, alteration or disclosure. Access is limited to people who need the information for their work, with confidentiality requirements and appropriate controls over service providers. We investigate suspected breaches and notify the regulator and affected individuals where the law requires.

10 How long we retain information

We keep identifiable information only for as long as necessary. The period depends on the type of record, our relationship, applicable legal duties and any live dispute. Our standard periods and criteria are:

Record	Retention period or criteria
Routine candidate and relationship records	Normally two years from our last meaningful two-way contact, then deleted or anonymised unless a documented, time-limited legal or business need justifies longer retention. An unanswered marketing email does not restart this period.
Placement, contract and transaction records	Necessary records are typically retained for six years from the relevant transaction or end of the engagement, to support accounting, compliance and legal claims. This does not mean every document in a candidate file is kept for six years.
Statutory and sensitive records	Tax, payroll, right-to-work and other legally required records follow the applicable statutory period. Sensitive and criminal-record material is kept for the shortest period justified by the check or duty, with restricted access.
Events, subscriptions and preferences	Event administration records are kept while needed for the event and reasonable follow-up. Subscription and community details are kept while participation continues or otherwise needed, and reviewed for inactivity. A minimal suppression record may be kept to respect an opt-out.
Complaints, disputes and security records	Retained as needed to investigate, demonstrate our response and meet applicable legal or limitation requirements. A documented legal hold may delay deletion; records are reviewed when that need ends.

We may retain genuinely anonymised statistics, which no longer identify you. Ask our privacy lead about the period applying to a particular record.

11 Communications and website privacy

Recruitment and marketing messages. We contact candidates about recruitment services and suitable opportunities and business contacts about relevant services, insights and events. Some vacancy messages are direct marketing, so we apply the applicable marketing rules as well as the UK GDPR.

Where required by the Privacy and Electronic Communications Regulations, we obtain consent before sending electronic marketing. We rely on an existing-customer exception only where all its conditions are met. Relevant marketing to corporate subscribers may rely on legitimate interests without prior electronic-marketing consent, but individuals retain the right to object. Different rules apply to sole traders and some partnerships. Public contact details do not automatically authorise marketing.

You can stop marketing at any time using an unsubscribe option or by contacting us. This does not prevent necessary administrative messages about an active application, assignment or contract. We keep a minimal suppression record where needed so that you are not added back to marketing lists.

Events and professional communities. We use registration, contact and participation information to organise events and communities, including SHIIIFT, and communicate about participation. Separate promotional communications follow the marketing rules above. If you choose to join a group on a third-party messaging platform, your profile or contact details may be visible to other members, depending on the service and settings. We explain relevant sharing before you join; joining is optional.

Call recordings and transcripts. We may keep relevant notes of calls and meetings. If we propose to record or transcribe a call, meeting or event, we will first explain the purpose, lawful basis, recipients, retention and available choices. Any use of AI tools must be covered by appropriate transparency and safeguards. This notice does not provide blanket consent to recording or AI processing.

Website forms and technical information. We use information you submit through recruitwithpurpose.co.uk to answer enquiries, manage applications and provide requested services. Necessary technical logs may be used to operate and secure the website, relying on legitimate interests.

Cookies and similar technologies. These technologies can store or access information on your device. Where consent is required, we will seek it before the technology operates and provide clear information about its purpose, provider and duration. You must be able to refuse or withdraw consent as easily as you give it. Where a statutory exception applies, we meet its conditions, including any required information and simple means of objecting. Using our website does not itself give consent to optional tracking or marketing.

You can contact us for information about current website technologies and how to manage preferences. Browser controls can also manage cookies, although blocking necessary cookies may affect website features. External websites and platforms operate under their own privacy information.

12 Automated decisions

Our recruitment decisions involve human consideration. We do not make decisions about you based solely on automated processing that produce legal or similarly significant effects. If this changes, we will provide information about the processing, its likely consequences and the safeguards available, including human intervention, representations and a way to challenge the decision, before introducing it.

13 Your rights and choices

Your rights depend on the purpose and lawful basis. Subject to applicable conditions and exemptions, you may ask us to:

- Provide access to your personal information and information about how we use it.
- Correct inaccurate information or complete missing information.
- Erase information where there is no lawful reason to retain it, or restrict its use in the circumstances provided by law.
- Provide information you supplied in a structured, commonly used, machine-readable format, or transmit it to another controller where technically feasible, when processing is automated and based on consent or a contract with you.

Your right to object. You can object to processing based on legitimate interests for reasons relating to your situation. We will stop unless we demonstrate compelling legitimate grounds overriding your interests, rights and freedoms, or the information is needed for legal claims. Your right to object to direct marketing, including related profiling, is absolute: we will stop that use when you object.

Withdrawing consent. Where we rely on consent, you can withdraw it at any time, as easily as you gave it, by contacting us or using the relevant preference control. Withdrawal does not affect processing that was lawful before withdrawal. We may still need to retain specific information for a separate legal purpose, which we will explain.

Making a request. Contact contact@recruitwithpurpose.co.uk or our privacy lead using section 1, or write to our registered office. You do not need to quote the law or use a particular form. We may ask for proportionate identity checks or clarification where necessary.

We respond without undue delay, normally within one month. Where the law allows, this may be extended by up to two further months for complex or multiple requests, or the time limit may pause while necessary clarification is sought. We will explain any lawful extension or pause and the reasons. Requests are normally free; we may charge a reasonable fee or refuse a manifestly unfounded or excessive request only where permitted, and will explain our decision and your options.

14 Questions and complaints

If you are concerned about how we handle your information, contact our privacy lead or email contact@recruitwithpurpose.co.uk. Please describe the issue and any outcome you seek. We accept complaints through other reasonable channels too; you do not have to use a form or legal wording.

We will acknowledge your complaint within 30 days, make appropriate enquiries without undue delay, keep you informed and tell you the outcome without undue delay. If your complaint concerns the privacy lead, you may contact James Ivall at james@recruitwithpurpose.co.uk.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK data protection regulator. The ICO generally expects you to raise your concern with the organisation first. This does not remove your legal right to complain to the regulator or seek a remedy through the courts.

ICO complaints: ico.org.uk/make-a-complaint

15 Changes to this notice

We review this notice regularly and update it when our processing or the law changes. The version and update date appear on the first page. We will draw material changes to your attention where appropriate and provide any additional information required before using your information for a new purpose.