

Data Protection Policy

Recruit with Purpose Limited

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

1 Purpose and scope

Recruit with Purpose Limited (RWP) must handle personal information lawfully, fairly, securely and transparently. This policy sets the working rules for our directors, employees, workers, contractors and anyone authorised to handle information on RWP's behalf. It covers electronic and paper records, recruitment systems, email, messaging, remote work and approved technology.

It applies to information about candidates, workers, clients, suppliers, referees, website and event users, job applicants and our own staff. The applicable framework includes the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations (PECR), as amended, including by the Data (Use and Access) Act 2025.

Read this alongside RWP's Privacy Policy and any employee privacy notice. Privacy notices explain our processing to individuals; this policy establishes the controls staff must follow. A new use of information must be assessed and reflected in the relevant notice before it starts.

2 Accountability and contacts

Henry Ivall, Director, is the privacy lead and policy owner. James Ivall, Director, is the alternative contact. Directors are responsible for oversight, resources, training, lawful processing decisions, rights requests, complaints and breach response. A privacy-lead role does not itself constitute appointment of a statutory Data Protection Officer (DPO); directors must review whether the legal requirement for a DPO applies.

Privacy enquiries: contact@recruitwithpurpose.co.uk

Primary contact: Henry Ivall, Director — henry@recruitwithpurpose.co.uk

Alternative contact: James Ivall, Director — james@recruitwithpurpose.co.uk

Staff must follow approved procedures, use information only for authorised work, complete training and report mistakes, suspected breaches and requests immediately. Managers must ensure access is appropriate and that concerns reach the privacy lead promptly.

3 Core principles

- Lawfulness, fairness and transparency: identify a valid legal basis and explain the use of information clearly.
- Purpose limitation and minimisation: collect only what is needed for a defined purpose and assess any proposed new use.
- Accuracy and storage limitation: correct errors promptly and keep information only for a justified period.
- Security and accountability: protect confidentiality, integrity and availability, and keep evidence of compliance.

The privacy lead must maintain appropriate processing records, retention rules, assessments, supplier records and incident logs, and keep the ICO fee registration current where required. Decisions and exceptions must be documented, not assumed.

4 Lawful collection and use

Before collecting or using information, identify the purpose, necessary data, legal basis, source, recipients and retention period. Give the relevant privacy information when collecting directly. For information obtained indirectly, provide it within the legal period, normally within one month, or at first contact or disclosure if earlier, unless a documented exception applies.

Basis commonly used by RWP	Required approach
Legitimate interests	Assess and record the purpose, necessity and balance with the person's rights. Ordinary candidate matching or business relationship management is not exempt from this assessment.
Contract	Use only where necessary for a contract with the individual, or specific steps they request before entering one. A contract with a client organisation does not by itself provide this basis for a candidate's data.
Legal obligation	Identify the applicable duty, such as relevant payroll, tax or right-to-work requirements. Collect only the information needed to meet it.
Consent	Obtain a freely given, specific, informed and unambiguous choice where relied on; record it and make withdrawal easy. Do not use consent where refusal cannot be respected.

Other statutory bases may apply in limited circumstances and require the privacy lead's assessment. Do not assume that a public profile, a supplied CV or agreement to a role gives unrestricted permission to use or share personal information.

5 Sensitive information and recruitment checks

Health, racial or ethnic origin, religion, sexual orientation, trade-union membership and other special category information require both an Article 6 lawful basis and a valid Article 9 condition. Where required, identify the relevant Data Protection Act 2018 Schedule 1 condition and maintain an appropriate policy document before processing.

Criminal allegations, convictions and related information have separate Article 10 protections. The privacy lead must verify the legal authority or Schedule 1 condition, necessity and safeguards before any criminal-record check. Use only a check permitted for the role; consent alone does not remove these requirements.

Limit checks to the role and stage of recruitment. Avoid unnecessary identity documents or sensitive details in CVs sent to clients. Confirm the candidate understands the proposed submission and record their agreement to representation; this is a business safeguard, not automatically the GDPR lawful basis. Keep adjustment and equality-monitoring information restricted and separate from selection decisions where appropriate.

6 Marketing, cookies and recordings

Check both UK GDPR and PECR before sending marketing, including job alerts or event promotions. Record consent where PECR requires it; legitimate interests do not override that requirement. Identify the sender, provide a simple opt-out, honour objections and maintain a minimal suppression record. Do not treat all business email addresses alike: sole traders and some partnerships have individual-subscriber protections.

Assess website cookies and similar technologies and obtain consent unless a valid statutory exemption applies. Before recording, transcribing or using AI tools with personal information, obtain the privacy lead's approval, assess risks and provide clear information about the purpose, legal basis, recipients, retention and any genuine choice.

7 Sharing, suppliers and international transfers

Share information only with authorised recipients who need it for a documented, lawful purpose. Check the recipient, attachment and permissions before sending; use an approved secure method. Send only relevant candidate information to a client, and protect referee and third-party information.

Establish each recipient's role. A processor acting only on RWP's instructions needs an Article 28-compliant contract, proportionate security checks and appropriate subprocessor controls. Clients, employers or payroll providers may instead be independent controllers; assess the actual arrangement and document suitable sharing safeguards. Agree Article 26 responsibilities where parties are joint controllers.

Before personal information is transferred or made accessible outside the UK in a restricted transfer, the privacy lead must confirm an applicable UK adequacy arrangement, or appropriate safeguards such as the UK IDTA or UK Addendum with the required data protection test, commonly called a transfer risk assessment. Use exceptions only where their legal conditions are met; a supplier's overseas location or contract alone is not sufficient.

8 Security and everyday handling

- Use approved accounts, systems and storage. Do not send work data to personal email, copy it to unapproved drives or enter it into unapproved AI or other services.
- Grant access on a need-to-know basis; review permissions and promptly remove access when roles change or someone leaves. Use strong unique passwords, multi-factor authentication where available and secure device locking.
- Keep devices and software supported and updated, use appropriate encryption, protect paper records and avoid exposing personal information in shared spaces. Verify unusual requests through a trusted channel.
- Maintain appropriate backups and recovery arrangements; check that information can be restored. Dispose of records and equipment securely through approved methods.

Directors must ensure technical and organisational measures are proportionate to the risks and are reviewed regularly. Staff must report lost equipment, misdirected messages, suspicious access or unavailable/corrupted data immediately, including when working remotely.

9 Retention and deletion

Record category	Retention rule
Ordinary candidate and relationship records	Normally two years from the last meaningful two-way contact. Then delete or anonymise unless a documented, time-limited need justifies retention. Unanswered marketing does not restart the period.
Necessary placement, contract and transaction records	Typically six years from the relevant transaction or end of the engagement, subject to the applicable legal requirement or claim period. This does not justify keeping the whole candidate file.
Employee, payroll and right-to-work records	Apply the specific statutory and employment retention schedule for each record type; no single period covers all staff records.
Sensitive data and other records	Keep for the shortest justified period under the retention schedule. Restrict access and document any legal or investigation hold.

Review active client records for continuing need. Apply deletion to working copies and suppliers where appropriate; manage backups through their documented cycle. Review holds regularly and delete or anonymise when the reason ends. Keep a record of material retention decisions.

10 Individual rights and complaints

People may request access, correction, deletion, restriction or portability, object to processing, or withdraw consent where it is used. The scope depends on the circumstances. Portability applies to qualifying automated processing based on consent or contract. A direct-marketing objection must be honoured; other objections require the applicable assessment.

Forward any request to the privacy lead immediately, even if made verbally or without mentioning data protection. Record its receipt date, verify identity proportionately and preserve relevant information. Do not delete or conceal information to avoid disclosure. Only the privacy lead may apply exemptions or refuse a request, with reasons and appropriate advice.

Respond without undue delay and normally within one month. A lawful extension of up to two further months for complexity or multiple requests must be explained within the initial month. Apply any permitted pause for necessary clarification or identity information only where the legal conditions are met and record the calculation. Responses are normally free of charge.

Accept privacy complaints through the published contacts. Acknowledge them within 30 days, make appropriate enquiries, keep the person informed and communicate the outcome without undue delay. Record the complaint and remedial action. Explain the right to complain to the Information Commissioner's Office at ico.org.uk; internal handling must not obstruct that right.

11 Personal data breaches

A breach can involve accidental or unlawful loss, destruction, alteration, disclosure, access or loss of availability. Report an actual or suspected breach immediately to Henry or, if unavailable, James. Give known facts, the time discovered, affected records and any containment already taken. Do not wait until you have all the details.

The privacy lead must promptly contain the incident, preserve evidence, assess risks to people and record the breach, decisions and corrective action. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to pose a risk to individuals' rights and freedoms. Provide information in phases if necessary and explain any delay.

Where a breach is likely to pose a high risk, inform affected people directly without undue delay unless a lawful exception applies. Explain what happened, likely consequences, protective steps and a contact. If RWP acts as a processor, notify the relevant controller without undue delay. Document every breach, including reasons for not notifying.

12 New processing, training and review

Build privacy into new systems and activities. The privacy lead must assess proposed changes and complete a data protection impact assessment before processing likely to create high risk; consult the ICO where required if high residual risk cannot be reduced. Do not introduce solely automated recruitment decisions with legal or similarly significant effects: RWP requires meaningful human assessment and a route to challenge decisions.

Provide induction and proportionate refresher training, maintain records and review compliance. Unauthorised handling or deliberate misuse may lead to disciplinary action following a fair process. Review this policy at least annually and after material changes in law, processing or risk, or a significant incident.

Policy owner: Henry Ivall, Director. Next scheduled review: 21 October 2027.