Candidate Recruitment Policy

At English Provender Company (EPC), we are committed to running a fair, transparent and people-first recruitment process. This policy explains how we collect, use and protect candidate information throughout the hiring journey, in line with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA). This policy covers both EPC sites: Newbury and Newport

1.0 Scope

This policy covers only the personal data of job applicants (direct applicants, internal applicants, agency-submitted candidates, internal referrals, proactively sourced applicants, and applicants sourced by any other lawful means). It does not apply to employee data, customer data or any other personal data processed by the Company for business operations. It does not replace EPC's wider Data Protection/UK GDPR policy.

1.1 Legal framework

We are committed to meeting our responsibilities under UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA), including updates that took effect in February 2026 and June 2026.

1.2 Roles and responsibilities

EPC has appointed Hannah Sheldon, Head of People as the Data Protection Officer (DPO). The DPO informs and advises EPC on data protection obligations. Questions about this policy or requests for further information should be directed to your site HR team or the DPO (see Section 10.3).

2. Types of data we collect

During the recruitment process, EPC collects and processes only the personal data necessary for assessing a candidate's suitability for employment.

2.1 Application information

CVs (including contact details), application forms, cover letters and any materials submitted as part of an application.

2.2 Personal contact details

Name, address, email address, telephone number and other details required to communicate with you during the recruitment process.

2.3 Assessment and interview information

Qualifications, skills, employment history, professional experience, interview notes, assessment results/scores and selection documentation.

2.4 Right to work documentation

Identification and immigration documents required to verify legal entitlement to work in the UK (processed under legal obligation).

2.5 Equal opportunities monitoring data (special category)

Information voluntarily provided for monitoring equality, diversity and inclusion, such as gender, ethnicity or disability. This information is processed under specific legal conditions and is not used in decision-making.

2.6 Reasonable adjustment information (special category)

Limited information a candidate may choose to share to request adjustments for interviews or assessments. Used only to support participation and handle appropriate safeguards.

2.7 Background check information

Where relevant and lawful, pre-employment checks such as references, criminal records checks (where legally justified), or professional verifications such as qualification certificates.

2.8 Communications

Messages and scheduling communication between candidates and EPC (e.g., interview arrangements and status updates).

2.9 CCTV

If you are invited to an onsite interview, please be aware that we have site-wide CCTV, which may capture your image when attending interviews or other onsite activities. CCTV is processed under legitimate interest (security, health and safety and incident management prevention) and recognised legitimate interest (crime prevention and crime detection). Access to CCTV recordings is strictly monitored and footage is normally retained for 1 month and will only be shared or retained longer when required by law or legitimate business reasons. CCTV is not used as part of the recruitment decision making process.

These categories (2.1 to 2.8))are recognised as standard and necessary for conducting a lawful and proportionate recruitment process and CCTV (2.9) is a separate site wide measure and is not part of the recruitment process, it may incidentally capture your image when you attend our premises.

3.0 Legal basis for processing

3.1 Contract

We process personal data where it is necessary to take steps to enter into an employment contract.

3.2 Legal obligation

We process certain information because we are legally required to do so. This includes:

- Confirming right to work and verifying identity documentation
- Meeting statutory requirements under UK employment and immigration law
- Completing safeguarding or regulatory checks where required
- If you choose to tell us about the requirement for reasonable adjustment due to health conditions or a disability during the recruitment process. Although you may choose to tell us about this information, we do not rely on consent.

These legal responsibilities form part of EPC's statutory duties during recruitment.

3.3 Legitimate interests

We process candidate data where it is necessary for EPC's legitimate interests in running an efficient, fair and secure recruitment process. This includes:

- Reviewing applications, qualifications, assessing suitability, shortlisting and making offers
- Arranging interviews/communication
- Maintaining recruitment and audit records
- Ensuring system and data security
- Gaining references
- CCTV: security, health and safety, incident prevention or linked investigations
- Equal opportunities monitoring

When we rely on legitimate interests to process candidate information, we ensure this is done fairly and proportionately and does not override your rights (balancing test applied).

3.4 Recognised legitimate interests

Data protection law introduced a small number of processing activities that organisations may carry out under recognised legitimate interests—such as crime prevention or ensuring network and information security. These are limited in scope and do not generally apply to standard recruitment activities. EPC does not rely on recognised legitimate interests for routine recruitment processing; instead, we use the standard legitimate interest's basis with a balancing test. Where required, EPC may share personal data with law enforcement agencies for the prevention or detection of crime, as permitted under data protection legislation (including the Data Protection Act 2018 crime exemption).

In addition to the above, we operate CCTV at our sites for prevention and detection of crime under recognised legitimate interest. This does not form part of routine recruitment processing.

3.5 Consent

We rely on consent only where the candidate has a genuine choice and the processing is optional, for example: optional communications. We do not rely on consent for core recruitment decisions.

4. Special category data

4.1 Examples

- If you choose to tell us about a health condition or disability so we can make reasonable adjustments during the recruitment process, we will use this information solely to support you. We process this data to create a fair and accessible recruitment experience and to meet our legal obligations under the Equality Act 2010. This processing is carried out under the lawful basis of legal obligation Article 6(1)(c) UK GDPR) and employment and social protection law (Article 9(2)(b) UK GDPR and Schedule 1, Part 1(1) Data Protection Act 2018)

- We process equality-monitoring information under our legitimate interests in promoting fairness, diversity and equal opportunities. Because this includes special category data, we rely on the substantial public interest condition for equality of opportunity or treatment (Article 9(2)(g) UK GDPR and Schedule 1 of the Data Protection Act 2018).

Processing of special category data always requires additional protection and is handled with strict confidentiality.

5. How we use candidate data

We use your personal information only for purposes that help us run a fair, safe and effective recruitment process. We limit the information we collect, use it only when necessary, and keep it only for as long as it is relevant to assessing your application and moving you through the recruitment journey. We may:

- Review your application (CV, cover letter, portfolio or supporting information)
- Understand your experience, skills, qualifications and suitability for the role applied for and conduct screening calls where appropriate
- Arrange and schedule interviews and contact you about each stage
- Carry out assessments, tests or other evaluation exercises where required
- Verify your identity and conduct right-to-related work checks (required by UK law)
- Maintain accurate recruitment records to demonstrate fairness, consistency and compliance
- Make hiring decisions (shortlisting, assessment outcomes and final decisions)
- Communicate with you about the outcome of your application
- Respond to legal, insurance or regulatory requests, where required
- Meet safeguarding, security and compliance requirements, including detecting or preventing fraud or misconduct
- Manage interview logistics (e.g., arranging site access or providing reasonable adjustments)
- Monitor the effectiveness and fairness of our recruitment process (using anonymised or aggregated data wherever possible)

- Contact you about future opportunities, where appropriate and only within lawful retention periods
- Protect our systems and premises, including basic security and access management relevant to interviews or assessments
- Comply with record-keeping duties under employment and immigration law
- Carry out any other processing required for the recruitment process only

We only use your data when it is necessary, proportionate and relevant to your application (data minimisation principle).

6. Automated decision-making and digital tools

EPC does not use automated decision-making, AI systems or algorithmic tools to make hiring decisions. All decisions about your application are made by people.

6.1 Transparency and safeguards (if tools are introduced)

- We will explain how any digital system operates if tools are introduced
- We will maintain meaningful human oversight over all recruitment decisions
- You will have the right to request a human review of any decision that affects you
- You can raise concerns through our internal data protection complaints process and they will be investigated fairly and promptly

At present, EPC's recruitment remains fully human-led; this section is provided for transparency under updated UK data protection law.

7. Data sharing

We only share your personal information when it is necessary, proportionate and directly connected to the recruitment process. Any organisation we share your data with must protect it and use it only for the purpose we instruct. We do not sell your data.

7.1 We May Share Your Data With:

- Hiring managers and HR teams (this may include the wider Billington Group) involved in reviewing your application and making decisions
- Recruitment agencies acting on our behalf
- Assessment and testing providers, if assessments form part of the recruitment process
- Right to work and identity verification services, as required by UK law
- IT providers who host or support our recruitment systems securely
- If you visit our site, CCTV may capture your image. We may use this footage for health and safety, security, crime prevention and incident-management purposes, including investigating accidents or complying with health and safety reporting duties. We may share this information with insurers, legal advisors or law-enforcement authorities where necessary.
- Occupational health services (only where relevant, e.g., adjustments or role-specific health requirements)
- Referees, educational bodies or professional organisations for verification
- Professional advisers (e.g., legal advisers when required)

- Regulators, courts or the police, but only when the law requires it or where necessary to prevent or detect a crime

8. Data retention

We keep your personal information only for as long as it is genuinely needed for recruitment, audit, fairness and legal purposes. We do not keep candidate information for longer than necessary.

8.1 Unsuccessful applicants

Retained for 6 months after the recruitment process concludes (to respond to legal claims, maintain fair records, meet audit requirements and consider for other internal opportunities).

8.2 Successful applicants

If you are offered and accept a role, your recruitment information will be moved to your employee HR file and managed under our Employee Privacy Notice.

8.3 Longer retention

We may keep certain information for longer only where required by law (for example, to meet regulatory or legal obligations). Retention beyond what is necessary is not permitted, in line with UK GDPR's storage limitation principle.

8.4 Talent pool

If an unsuccessful candidate would like to be considered for opportunities after the standard 6-month retention period, they must give us their *explicit consent* to keep their details for an additional 12 months. Consent is fully optional, and candidates may withdraw it at any time. If consent is not provided, the standard 6-month retention and deletion rules apply.

9. Your rights

9.1 Right of access (DSAR)

You can ask us for a copy of the personal information we hold about you.

9.2 Right to correction

If any of your data is inaccurate or incomplete, you can ask us to correct it.

9.3 Right to erasure (in certain circumstances)

You can ask us to delete your information. This does not apply where we must keep data for legal or regulatory reasons.

9.4 Right to restrict processing

You can ask us to limit how we use your data in specific situations—for example, if you believe it is inaccurate or being processed unlawfully.

9.5 Right to object

You may object to processing based on legitimate interests unless we have strong grounds to continue.

9.6 Rights linked to automated decisions

EPC does not use automated decision-making for hiring. If this ever changes, you will have the right to receive an explanation and to request a human review and express your point of view.

9.7 DSAR Response times and approach

We will complete searches that are reasonable and proportionate when responding to DSARs within 1 month of receiving your request. We may pause ('stop the clock') while we wait for clarification from you or if we need more information to verify your identity. If a request is complex, or you make several requests, we may take up to an extra two months to respond. If this happens, we will let you know and explain why.9.8 How to Make a DSAR

You can make a request for your personal data at anytime by contacting us on the email address below:

Email: info@englishprovender.com or epchrnewbury@englishprovender.com

Head office address: English Provender Company, Greenhand Business Park, Thatcham, Berkshire, RG19 6HA

- Acknowledge your request
- Clarify anything we need (if required)
- Carry out reasonable and proportionate searches
- Provide your information securely
- Explain anything that may affect the timeframe

We aim to make the process as smooth and transparent as possible, in line with UK GDPR, the Data Protection Act 2018 and DUAA reforms introduced in February and June 2026

10. Complaints handling (from 19 June 2026)

10.1 Internal complaints process

From 19 June 2026, EPC offers a formal internal data protection complaints process before concerns are escalated to the Information Commissioner's Office (ICO). Candidates can raise worries about how their personal information was collected, used, shared or retained during recruitment. We will investigate fairly, promptly and transparently, keeping you informed throughout.

10.2 Escalation to the ICO

If you remain unhappy after our internal review, you may then contact the ICO. Under the June 2026 DUAA changes, organisations must offer an internal process first; after that you have the right to escalate to the ICO.

10.3 Contact details

Data Protection Officer: Hannah Sheldon
Phone: 01635 528800
Email: Info@englishprovender.com or epchrnewbury@englishprovender.com

11. Data security

We take the security of your personal information seriously. EPC uses a combination of technical and organisational measures to protect your data and ensure it is handled safely throughout the recruitment process, aligned with UK GDPR, the Data Protection Act 2018, and DUAA expectations.

11.1 Our measures include

- Access controls so only authorised people involved in recruitment can view your information
- Secure systems and encrypted storage, where appropriate
- Data minimisation: we only collect and keep the information we genuinely need
- Secure deletion once no longer required, in line with retention rules
- Restricted access to candidate information at all stages
- Ongoing review of our security measures to ensure they remain effective and appropriate

12. International data transfers

EPC does not transfer candidate data to countries outside the EEA. If this position changes, we will implement appropriate safeguards and update this policy.

13. Policy review

We review this policy regularly to ensure it remains up to date with UK law and ICO guidance. As the ICO updates guidance following DUAA changes, we will update this policy to reflect any new requirements so you always have accurate information about how your data is used and protected.