UK GDPR Data Protection and Privacy Policy

1. Purpose

JGA Recruitment Group Ltd (the Company) is committed to protecting personal data and respecting the privacy rights of candidates, workers, employees, contractors, clients, suppliers, referees, emergency contacts and other individuals whose personal data is processed by the Company.

This policy sets out the Company's approach to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable UK data protection legislation. It provides a framework for collecting, using, storing, sharing, retaining, deleting and protecting personal data in a lawful, fair, transparent and accountable manner.

The Company also recognises the Privacy and Electronic Communications Regulations 2003 (as amended) in relation to electronic marketing, cookies and similar technologies, and will monitor phased changes introduced by the Data (Use and Access) Act 2025 where they affect data protection, complaint handling, e-privacy or recruitment processing obligations.

Where the Company processes personal data in connection with offering recruitment services to individuals in the EEA/EU, or where the EU GDPR otherwise applies, equivalent EU GDPR transparency, rights, transfer and accountability requirements shall also be observed.

This policy must be read together with the Company's privacy notices, retention schedule, information security policies, data breach procedure, data subject rights procedure and any related recruitment, HR, payroll, supplier and complaints procedures.

2. Scope

This policy applies to all employees, directors, contractors, temporary workers, consultants and third parties who process personal data on behalf of the Company.

It applies to all personal data processed by the Company, whether held electronically, in paper format, in email, within recruitment platforms or CRM systems, within Microsoft 365, in HR and payroll systems, within supplier systems, or in any other approved business system.

It applies to all processing activities carried out as part of recruitment, candidate management, client engagement, employee administration, payroll, finance, marketing, supplier management, website enquiries, complaints handling and general business operations.

3. Definitions

Personal data means information relating to an identified or identifiable living individual. This includes names, contact details, identification information, employment history, CVs, interview notes, right-to-work information, payroll details, online identifiers and any other information that can identify a person directly or indirectly.

Special category data means more sensitive personal data, including information about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, and data concerning sex life or sexual orientation.

Criminal offence data means personal data relating to criminal convictions, offences, allegations, proceedings or related security measures. This must only be processed where a valid lawful basis and a specific legal condition are documented.

Processing means any operation performed on personal data, including collection, recording, storage, use, consultation, sharing, disclosure, restriction, erasure or destruction.

The Company may act as a data controller where it determines why and how personal data is processed. It may also act as a processor where it processes personal data on documented instructions from a client or other controller.

4. Data Protection Principles

The Company shall process personal data in accordance with the UK GDPR principles. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; retained only for as long as necessary; and protected through appropriate security measures.

The Company shall also comply with the accountability principle by being able to demonstrate compliance through appropriate policies, records, training, risk assessments, supplier due diligence, retention controls, breach records, data subject rights records and management oversight.

5. Roles and Responsibilities

The Company's current data protection contact is the Operations & Sustainability Director. The Company shall ensure that this contact route remains current, published and supported by a responsible senior person or Data Protection Lead who oversees privacy compliance, coordinates data protection activities, monitors controls, supports data subject rights requests, assists with breach investigations, advises on changes to data protection requirements and ensures appropriate training is provided.

The Company does not need to describe this role as a Data Protection Officer unless it has formally appointed a statutory DPO. If a statutory DPO is appointed in future, the Company must meet the additional UK GDPR requirements that apply to that role.

Managers are responsible for ensuring that personal data handled within their areas is processed in accordance with this policy. All staff are responsible for protecting personal data, only accessing data needed for their role, reporting suspected breaches immediately and completing required training.

6. Lawful Basis for Processing

The Company shall identify and document an appropriate lawful basis under Article 6 UK GDPR before processing personal data. Depending on the context, the lawful bases may include performance of a contract,

steps prior to entering into a contract, compliance with a legal obligation, legitimate interests, consent, vital interests or public task where applicable.

Legitimate interests may be used where processing is necessary for a genuine business purpose and the Company has considered and balanced the interests, rights and freedoms of the individual. Examples may include recruitment administration, candidate relationship management, client relationship management, network and information security, business continuity and limited direct business-to-business communications where permitted by law.

Consent shall only be relied upon where it is freely given, specific, informed and unambiguous. Where consent is used, the Company shall keep evidence of consent, allow withdrawal as easily as consent was given, and avoid using consent where another lawful basis is more appropriate.

7. Special Category and Criminal Offence Data

The Company shall only process special category data where an Article 6 lawful basis and an Article 9 condition are identified and documented. Examples may include employment law obligations, assessment of working capacity, explicit consent, legal claims or substantial public interest where applicable.

Where criminal offence data is processed, including DBS or background check information, the Company shall identify a lawful basis, confirm a permitted condition under UK law, limit access, retain only what is necessary and document the relevant safeguards.

Special category and criminal offence data must be subject to stricter access controls, minimisation, retention and secure disposal requirements.

8. Categories of Personal Data Processed

The Company may process personal data relating to candidates, applicants, workers, contractors, employees, former employees, client contacts, supplier contacts, referees, emergency contacts, website users and complainants.

Personal data may include contact details, CVs, work history, qualifications, interview notes, right-to-work information, passport or identification information, payroll data, bank details, tax details, emergency contact details, references, communications, role preferences, marketing preferences, system logs and records required for legal, recruitment, contractual or operational purposes.

The Company shall ensure that data mapping and records of processing activities are maintained at a level proportionate to the size, nature and risk of the processing undertaken.

For website users, the Company may process technical information such as IP address, browser type and version, operating system, platform, URL clickstream, page response times, download errors, page visit duration and methods used to browse away from the website, where required for website operation, analytics, security, troubleshooting and service improvement.

9. Privacy Notices and Transparency

The Company shall provide clear, accessible and up-to-date privacy information at the point personal data is collected, or as soon as reasonably practicable where personal data is received from another source.

Privacy information shall explain what personal data is collected, why it is used, the lawful basis relied upon, who it may be shared with, international transfers, retention periods, individual rights, complaint routes and how to contact the Company about data protection matters.

Recruitment adverts, candidate registration forms, website forms and onboarding documentation should include or link to relevant privacy information and should make clear how long candidate information may be retained where retention is based on consent or legitimate interests.

Where personal data is obtained from third-party sources such as LinkedIn, corporate websites, job boards, online CV libraries, business cards or personal recommendations, the Company shall provide the required privacy information within a maximum of 30 days, unless an exemption applies, including the source of the data and whether it came from publicly accessible sources.

10. Data Subject Rights

Individuals have rights under UK GDPR, subject to exemptions and limitations. These include the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights relating to automated decision-making and profiling.

Requests may be made verbally or in writing and do not need to refer to UK GDPR by name. Staff must forward any suspected rights request to the Data Protection Lead without delay.

The Company shall verify the identity of the requester where appropriate, clarify the scope of the request where necessary, respond within one month unless an extension is permitted, and keep a record of the request, decision and response. No fee shall be charged unless the request is manifestly unfounded or excessive, or repeated copies are requested.

11. Subject Access Requests

Subject Access Requests (SARs) must be handled promptly and in accordance with UK GDPR. The Company shall acknowledge receipt, verify identity where required, identify relevant systems and records, review personal data, apply exemptions where lawful, redact third-party information where appropriate and provide the response securely.

Before sending SAR information, the Company shall confirm the appropriate delivery method and destination with the requester, particularly where the request has been received from a work email address, shared mailbox or representative.

Where searches involve email, CRM, Microsoft 365, SharePoint, HR folders or other systems, the Company shall take reasonable and proportionate steps to locate relevant personal data. Search criteria, systems checked and exemptions applied should be recorded.

12. Data Protection Complaints

The Company shall maintain a standalone process for handling data protection complaints. A data protection complaint is where an individual states or indicates that they are unhappy with how the Company has handled their personal data or complied with data protection law.

The Company must give individuals a clear way to raise a data protection complaint. Data protection complaints may be directed to the Operations & Sustainability Director as the confirmed data protection contact, unless a dedicated complaints route is published separately.

The Company shall acknowledge receipt of data protection complaints within 30 days, take appropriate steps to investigate and respond without undue delay, keep the complainant informed where appropriate, and provide the outcome without undue delay. Individuals must also be told of their right to complain to the Information Commissioner's Office if they remain dissatisfied.

13. Data Retention and Disposal

Personal data shall be retained only for as long as necessary for the purpose for which it was collected and in accordance with legal, regulatory, contractual and business requirements. Retention periods shall be documented within a retention schedule or equivalent record.

The Company shall periodically review personal data held in CRM systems, email, SharePoint, HR folders, recruitment platforms and paper records to ensure information is not retained longer than necessary. Duplicate or uncontrolled copies should be avoided where possible.

When personal data is no longer required, it shall be securely deleted, anonymised or destroyed using appropriate methods. Paper records containing personal data must be disposed of using confidential waste or secure shredding.

14. Data Security

The Company shall implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration or disclosure.

Controls may include access restrictions, password protection, multi-factor authentication, encryption, secure backup, secure file sharing, endpoint protection, patching, logging, confidential waste, clear desk and clear screen practices, staff training and incident reporting.

Access to personal data shall be limited to authorised personnel on a need-to-know basis. Personal data must not be stored on unmanaged personal devices or shared through unauthorised systems unless explicitly approved and protected by appropriate controls.

15. Data Sharing and Processors

The Company shall only share personal data where there is a lawful basis, a defined business need and appropriate safeguards. Personal data shall not be sold to third parties.

Where the Company uses suppliers or processors, it shall ensure that appropriate due diligence is completed and that written contractual terms are in place. Processor contracts must require processing only on documented instructions, confidentiality, security measures, assistance with rights requests and breaches, deletion or return of data, audit rights and controls over sub-processors.

Where the Company acts as a processor for a client, it shall process personal data only in accordance with the client's documented instructions and relevant contractual terms.

16. International Transfers

The Company may transfer personal data to service providers, clients or recruitment partners outside the UK and/or the EEA where necessary for recruitment services. Personal data shall only be transferred internationally where permitted by applicable data protection law and where appropriate safeguards are in place.

Safeguards may include UK adequacy regulations, the International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, EU Standard Contractual Clauses where the EU GDPR applies, binding corporate rules or another approved transfer mechanism. Transfer risk assessments and supplementary measures shall be completed where required.

Where recruitment activity involves overseas clients, candidates, employers of record, payroll providers, platforms or supplier systems, the Company shall maintain an understanding of the countries involved and the safeguards relied upon.

17. Privacy by Design and Data Protection Impact Assessments

The Company shall consider data protection at the start of new projects, services, systems, supplier relationships, recruitment processes, AI use cases or changes to processing activities.

A Data Protection Impact Assessment (DPIA) shall be completed where processing is likely to result in a high risk to individuals. Examples may include large-scale processing of sensitive data, systematic monitoring, new technologies, automated decision-making, AI-enabled profiling or processing involving vulnerable individuals.

DPIA actions shall be tracked until completed and unresolved high risks shall be escalated to senior management and, where legally required, the ICO.

18. Automated Decision-Making, Profiling and AI

The Company does not currently undertake solely automated decision-making or profiling that produces legal effects concerning individuals or similarly significantly affects them. Systems may be used to search, sort and identify information in accordance with parameters set by a person, but a person shall remain involved in recruitment and engagement decisions.

Individuals shall be provided with meaningful information about any solely automated decision-making that has legal or similarly significant effects, and their rights shall be respected. The Company shall not use unapproved AI tools to process candidate, employee, client or supplier personal data.

If significant automated decision-making is introduced in future, the Company shall provide appropriate information and safeguards, including human intervention, the opportunity for individuals to express their point of view and the ability to contest the decision where applicable.

AI, analytics or screening tools used in recruitment must be assessed for fairness, accuracy, bias, transparency, security, data minimisation and supplier compliance before use.

19. Marketing and Communications

Marketing activities involving personal data shall comply with UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations where applicable.

Marketing preferences, opt-ins, opt-outs and unsubscribe requests must be recorded and respected. Where consent is required, it must be specific and evidenced. Where legitimate interests are relied upon, the Company must ensure that the communication is necessary, proportionate and does not override individual rights.

The Company shall periodically review marketing lists and CRM records to ensure contact data remains accurate, relevant and lawfully retained.

20. Cookies and Similar Technologies

The Company's website may use cookies and similar technologies to distinguish users, enable website functionality, understand website usage and improve services. Where required by law, consent shall be obtained before placing non-essential cookies or similar technologies on a user's device.

Users must be provided with clear information about cookies and similar technologies and should be able to manage preferences through browser settings and, where available, the Company's cookie controls. Cookie and similar technology use shall comply with PECR and UK GDPR.

21. Personal Data Breaches

All suspected or actual personal data breaches must be reported immediately to the Data Protection Lead or responsible manager. Staff must not attempt to conceal or delay reporting a suspected breach.

The Company shall investigate breaches promptly, contain and remediate the issue, assess the risk to individuals, document the facts and decisions, and notify the ICO within 72 hours of becoming aware of a notifiable breach unless an exception applies.

Affected individuals shall be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms. Lessons learned shall be reviewed and corrective actions tracked.

22. Training and Awareness

All staff who process personal data shall receive appropriate data protection training at induction and at regular intervals thereafter. Training should cover recognising personal data, correct handling, data subject rights, SARs, data protection complaints, secure sharing, retention, breach reporting and acceptable use of systems.

Training completion should be recorded. Additional role-specific training should be provided for staff involved in recruitment, HR, payroll, marketing, finance, IT administration, SAR handling, complaints handling and supplier management.

23. Monitoring, Audit and Compliance

The Company shall periodically review compliance with this policy through proportionate checks, management review, supplier review, retention review, access review, data mapping updates and review of incidents, complaints and rights requests.

Non-compliance with this policy may result in disciplinary action, contract action, supplier escalation or other corrective measures. Where non-compliance creates a risk to individuals, it shall be managed as a data protection risk or incident.

24. Review

This policy shall be reviewed at least annually or sooner if there are significant changes to data protection law, ICO guidance, business operations, systems, suppliers, recruitment processes or the nature of personal data processed by the Company.

The Data Protection Lead shall maintain the review record and ensure that approved updates are communicated to relevant staff and, where appropriate, published externally.