Fraud Prevention and Response Policy

1. Policy statement

JGA Recruitment Group Ltd ("JGA" or "the Company") is committed to conducting its business with honesty, integrity and appropriate controls. JGA has zero tolerance for fraud, attempted fraud, deliberate concealment of fraud, or retaliation against a person who raises a genuine concern.

All suspected or alleged fraud will be assessed promptly and proportionately. Where appropriate, JGA may take disciplinary or contractual action, seek recovery of losses, notify clients, insurers, regulators or law-enforcement bodies, and pursue civil or criminal remedies.

2. Purpose

This policy sets out how JGA prevents, identifies, reports, investigates and responds to fraud. Its objectives are to protect candidates, workers, clients, suppliers, employees, company assets and information; support a culture in which concerns are raised early; and maintain proportionate fraud-prevention procedures.

3. Scope

This policy applies to all JGA employees, directors, contractors, temporary workers, job applicants, consultants, suppliers and other third parties acting for or on behalf of JGA. Relevant expectations may also be communicated to clients where their processes interact with JGA controls, including timesheet approval and verification of payment or worker information.

4. What JGA means by fraud

For this policy, fraud means dishonest or intentionally deceptive conduct intended to make a gain, cause or expose another person or organisation to loss, obtain an improper advantage, or conceal wrongdoing. Fraud can involve money, assets, information, identity, records, systems, services or reputation.

The Fraud Act 2006 provides for fraud by false representation, fraud by failing to disclose information where there is a legal duty to disclose, and fraud by abuse of position. This policy is broader operationally and also covers attempted fraud, collusion, forgery, deliberate manipulation of records, cyber-enabled fraud and deliberate hoaxes that are intended to produce a fraudulent outcome.

The Economic Crime and Corporate Transparency Act 2023 introduced a corporate offence of failure to prevent fraud for organisations within the statutory scope. Where that offence applies to JGA, the Company will maintain reasonable fraud-prevention procedures. Whether or not the statutory size threshold applies, JGA adopts proportionate prevention principles as a matter of good governance.

5. Responsibilities

5.1 Managing Director and Senior Management

Set the tone from the top and promote a culture in which fraud is not tolerated.

Ensure fraud risks are considered in business processes, material changes, client arrangements and third-party relationships.

Ensure appropriate prevention controls, training, reporting routes and investigation arrangements are maintained.

Decide, with appropriate professional advice where needed, whether matters should be reported externally or referred for disciplinary, contractual, civil or criminal action.

Ensure investigations are sufficiently independent, particularly where an allegation concerns a senior employee or a person who would normally investigate the matter.

5.2 Managers

- Understand the fraud risks within their area and ensure required controls are applied consistently.
- Escalate suspected fraud immediately and protect relevant records, documents and system evidence.
- Do not investigate serious allegations independently unless specifically authorised to do so.
- Ensure no person suffers retaliation for raising a genuine concern.

5.3 Employees, contractors and temporary workers

- Act honestly and comply with this policy and related procedures.
- Remain alert to unusual transactions, identity concerns, altered documents, unusual payment requests, data misuse and other fraud indicators.
- Report actual, attempted or suspected fraud promptly, including concerns involving colleagues, candidates, clients or suppliers.
- Co-operate with authorised investigations and preserve confidentiality.

A breach of this policy by an employee may result in disciplinary action up to and including dismissal, in accordance with the Company's disciplinary procedure. A contractor or temporary worker involved in fraudulent conduct may have their assignment terminated. JGA may also seek compensation or recovery where legally appropriate.

5.4 Job applicants

Applicants must provide information that is accurate, honest and complete and must not knowingly submit forged, altered, misleading or impersonated documentation. Material dishonesty or deliberate concealment may result in withdrawal of JGA's services, termination of an application or assignment, notification to a client where appropriate, and other lawful action.

5.5 Consultants, suppliers and other third parties

Third parties are expected to act with integrity and to comply with relevant contractual, anti-bribery, data-protection, information-security and fraud-prevention requirements. JGA may suspend or terminate dealings where fraud is established or where risk cannot be managed adequately.

6. Examples of fraud and fraud indicators

The following are examples only and are not exhaustive:

- Failure to account for money received, theft or embezzlement of Company, worker or client funds.
- Falsified expense claims, invoices, payroll records, commission records or accounting entries.
- Authorising or receiving payment for hours not worked; submission, alteration or collusive approval of false timesheets.
- Misappropriation or unauthorised alteration of contractor or temporary worker bank details, including fraudulent change-of-bank requests.
- Alteration, forgery or fabrication of identity documents, right-to-work evidence, qualifications, certificates, references or other candidate records.
- Providing deliberately misleading information or deliberately withholding information that is material to a recruitment, compliance, payment or client decision.
- Identity theft, impersonation, account takeover, phishing, business email compromise, cyber-enabled invoice fraud or unauthorised access to systems.
- Unauthorised amendments to databases, administration systems, CRM records, payroll systems or accounting records.
- Misuse, theft or unauthorised disposal of Company assets, data, intellectual property, credentials or confidential information.
- Receiving or offering gifts, services, payments or other inducements to obtain an improper advantage, including conflicts with the Anti-Bribery & Anti-Corruption Policy.
- Supplying free or reduced-cost services to friends, relatives or connected parties without proper authority.
- Collusion between employees, candidates, workers, clients or suppliers to circumvent controls or conceal wrongdoing.

7. Prevention and detection controls

JGA uses proportionate controls designed to reduce the opportunity for fraud and increase the likelihood that it is detected promptly. Controls include, where relevant:

- Periodic consideration of fraud risks and review of controls when processes, systems, services or material third-party arrangements change.
- Appropriate segregation of duties and authorisation limits for payments, refunds, credits, payroll and changes to financial records.

- Independent verification of requests to change bank or payment details using trusted contact information rather than relying solely on the message requesting the change.
- Review of financial transactions and accounting practices, including use of external accountants or auditors where appropriate.
- Examination of timesheets by experienced staff and validation of amendments. Amendments must be approved by an authorised client representative or submitted/approved through authorised secure systems.
- Receipts and supporting evidence for expenses, with reconciliation to approved claims.
- Candidate and worker due diligence, including identity, right-to-work, qualification, reference and other checks required by law, Company policy or client requirements.
- Checks that documents relate to the individual, are relevant to the check, are in date where applicable, and show no obvious signs of tampering. Copies and verification records must be retained in accordance with applicable retention rules.
- Appropriate DBS, credit or other security checks where lawful, proportionate and required for a specific role or client.
- Role-based system access, strong authentication, password controls, encryption and prompt removal or amendment of access when roles change or employment/assignments end.
- Secure storage and disposal of records containing personal, financial or confidential information, in line with the Data Protection and Information Security policies.
- Due diligence and proportionate contractual controls for suppliers, consultants and other associated persons.
- Fraud-awareness communication and training for relevant personnel, refreshed where risks or processes materially change.
- Management review of suspected control failures, trends, near misses and lessons learned.

8. Reporting suspected or alleged fraud

Anyone covered by this policy who knows of, suspects, or reasonably believes that fraud or attempted fraud may have occurred must report the concern as soon as possible. Do not wait for proof before reporting a genuine concern.

Where the concern involves the Managing Director, or where the reporter reasonably believes the normal reporting route is inappropriate, the concern should be raised through the Company's Whistleblowing Policy or with another appropriate senior person identified under that policy. External disclosures may also be protected by law in defined circumstances; individuals should follow the Whistleblowing Policy or obtain independent advice where needed.

Reports will be handled as confidentially as reasonably possible. JGA will not tolerate retaliation, victimisation or attempts to suppress a genuine report. Knowingly making a false or malicious allegation may itself be dealt with under the appropriate disciplinary or contractual process; an allegation that is not substantiated is not, by itself, evidence of bad faith.

9. Immediate actions when fraud is suspected

- Report the concern promptly using the route above.
- Preserve relevant emails, messages, documents, timesheets, financial records, audit logs and other evidence. Do not alter or delete records.
- Do not confront a suspected person, alert them to an investigation, or conduct covert enquiries unless specifically authorised.
- Do not communicate externally about the allegation unless authorised to do so.
- Where there is an immediate risk of further loss, data compromise or payment diversion, notify the appropriate senior manager so proportionate containment steps can be considered.

10. Assessment and investigation

The Managing Director, or an appropriately independent delegate where necessary, will assess the concern and determine the appropriate response. The response will be proportionate to the seriousness, credibility, financial or safeguarding impact, legal obligations, evidence-preservation needs and risk of continuing harm.

Investigations should be fair, documented and conducted on a need-to-know basis. Where specialist expertise or independence is required, JGA may use external legal advisers, accountants, forensic specialists, HR advisers or other appropriate professionals. JGA may suspend access, payments, assignments or duties on a precautionary basis where lawful and proportionate; such action is not a finding of wrongdoing.

Where appropriate, JGA may report matters to the police, Action Fraud or another competent authority, regulator, insurer, client or affected party. Decisions about external reporting should take account of legal obligations, contractual requirements, privilege, confidentiality, data protection and the need not to prejudice an investigation.

11. Outcomes and recovery

Where fraud or a serious control breach is substantiated, JGA may take one or more lawful actions, including disciplinary action, dismissal, termination of assignment or contract, withdrawal of services, recovery of money or property, civil proceedings, notification to relevant third parties, and referral to law-enforcement or regulatory bodies. Outcomes will be determined on the facts and in accordance with applicable procedures and law.

12. Records, confidentiality and data protection

JGA will maintain appropriate records of fraud reports, assessments, decisions, evidence, investigation steps, outcomes, losses and remedial actions. Records will be retained securely and only for as long as required by law, legitimate business needs and applicable retention policies. Personal data will be handled in accordance with the Company's Data Protection and Information Security policies.

13. Training, monitoring and review

Relevant personnel will receive fraud-awareness information or training appropriate to their responsibilities. Management will review significant incidents, near misses and control failures so that lessons learned are incorporated into processes, systems, due diligence and training.

This policy will be reviewed at least annually and sooner if there is a material change in legislation, regulatory guidance, business activities, fraud risk, systems or operating model.

14. Related policies and procedures

- Anti-Bribery & Anti-Corruption / Business Integrity
- Whistleblowing
- Disciplinary and Grievance
- Recruitment and qualification validation
- Eligibility to Work in the UK & Visa Status
- Referencing
- Data Protection
- Information Security
- Purchasing & Procurement
- Social Media
- Safeguarding
- Training