Data Protection Statement

Document type	Policy
Document owner	Ignite Talent Group Ltd
Approved by	Nicholas Ryan, Director
Date approved	12 June 2026
Next review	June 2027

This policy states the corporate position for clients, candidates, workers, suppliers and stakeholders as applicable.

Data Protection Statement

Ignite processes personal data relating to candidates, workers, clients, employees, referees, suppliers and website users. Recruitment activity routinely involves CVs, contact details, right-to-work evidence, qualifications, employment history, references and assignment information.

Purpose

This statement sets out Ignite's commitment to processing personal data lawfully, fairly, transparently and securely.

It should be read with the Privacy Notice, Information Security Policy and any candidate, worker, client or website privacy wording issued by Ignite.

Scope

This policy applies to Ignite Talent Group Ltd and to each Ignite recruitment vertical where the policy is relevant to its operations, client work, candidates, workers, consultants, employees and supply-chain relationships.

Where a vertical has a sector-specific requirement, that requirement should be read with the relevant appendix or operational procedure. Construction-specific controls are applied more rigorously where client sites, labour supply, temporary assignments, training evidence or framework onboarding require additional assurance.

Policy commitments

- Process personal data only where there is a lawful basis and a legitimate business or legal purpose.
- Tell individuals how their data is used through clear privacy information.
- Collect only data that is relevant and proportionate.
- Keep personal data accurate and update or correct it where required.
- Protect personal data against unauthorised access, loss, misuse or disclosure.
- Respect individual rights, including access, correction, deletion, restriction and objection where applicable.
- Report and manage personal data breaches promptly.

Responsibilities

Directors and senior leaders

- Set the policy direction, provide resources, and maintain accountability for the governance framework.
- Ensure material risks are reviewed and that controls remain proportionate to the size, risk profile and vertical activity of the group.

Managers and consultants

- Apply the policy in day-to-day recruitment, client, candidate and worker interactions.
- Keep records accurate and escalate gaps, concerns or client requirements promptly.

Employees, workers and representatives

- Act honestly, follow approved processes, protect confidential information and report concerns without delay.

How this policy is applied

Data controller position

Ignite Talent Group Ltd is the data controller for personal data processed through group governance and website functions. Where an Ignite group company processes data for its own recruitment activity, that company may act as a separate controller.

- Controller responsibilities must be reflected in privacy notices.
- Group entities should not be described as registered or as separate controllers unless the position is confirmed.

Candidate and worker data

Recruitment data may include CVs, employment history, contact information, right-to-work evidence, qualifications, training cards, references, role preferences, pay expectations, availability and assignment records.

- Collect data for recruitment, placement, assignment, compliance and client-introduction purposes.
- Share data with clients only where relevant, lawful and proportionate.
- Take care with special category data, criminal record information or health-related data.

Client and supplier data

Ignite processes contact, role, commercial and communication data relating to clients, hirers, suppliers, umbrella companies and professional contacts.

- Use client/supplier data for relationship management, contract performance, recruitment delivery and compliance.
- Keep business contact data secure and accurate.

Right-to-work and compliance records

Right-to-work documents, share codes, identity evidence and training records can contain sensitive identity information. These records must be handled securely and retained only for appropriate periods.

- Restrict access to staff with a clear business need.
- Do not send identity documents through informal channels unless approved and secure.
- Delete or archive records in line with retention rules.

Data breaches and subject rights

Any suspected data breach, misdirected email, lost device, unauthorised access or accidental disclosure must be reported promptly. Subject access requests must be escalated and not handled informally by individual consultants.

- Maintain breach records and decision logs.
- Respond to individual rights requests within legal timescales.

- Seek advice where a request is complex or involves third-party data.

Records and evidence retained

- Privacy notices and website privacy wording.
- Data processing and retention records.
- Subject access and individual rights request logs.
- Data breach log and actions taken.
- Processor and supplier due diligence records.
- ICO registration certificates and fee-payment evidence.

Sector-specific application

ICO registration

- Ignite Talent Group Ltd is registered with the Information Commissioner's Office under reference ZC135847.
- Ignite Engineering Talent Ltd is registered with the Information Commissioner's Office under reference ZC135854.
- Confirmed registration references are maintained in the Privacy Notice and internal compliance register.

Reporting concerns

Questions, concerns or requests for further information should be raised through the relevant manager or through the group compliance contact at compliance@ignitetalentgroup.co.uk.

Concerns involving wrongdoing, unsafe practice, exploitation, bribery, unlawful discrimination, data protection or serious non-compliance may also be escalated under the Whistleblowing and Speak-Up Policy.

Approval and review

Approved by	Nicholas Ryan
Position	Director
For and on behalf of	Ignite Talent Group Ltd
Date approved	12 June 2026
Approval method	Approved electronically
Next review	June 2027