Data Protection Policy

QBA Third-Party Supplier Policy

1. Purpose and Scope

QBA is committed to upholding the highest data protection and privacy standards with respect to all data it controls, including Personal Data belonging to QBA, its employees, customers, and other individuals. “Personal Data” means any information relating to an identified or identifiable natural person who can be identified directly or indirectly. This Policy applies to all third-party suppliers and vendors (“Suppliers”) who collect, access, store, transmit, or otherwise process Personal Data in connection with their engagement with QBA.

2. Applicability

The policy shall be applicable to all suppliers and vendors unless otherwise agreed.

3. Compliance Obligations

Suppliers shall:

- Comply with all applicable data protection laws, including, where relevant, the GDPR, UK Data Protection Act, and other local data protection legislation.
- Where acting as an independent controller, comply with the local laws governing the Personal Data they process.
- Where acting on QBA’s behalf, comply with QBA’s instructions, the applicable data processing agreement, and any standard contractual clauses incorporated into their contract with QBA.

4. Security and Processing Requirements

Suppliers shall:

- Process Personal Data only for the purposes specified by QBA.
- Implement appropriate technical and organizational measures to protect Personal Data against unauthorized access, loss, alteration, or disclosure.
- Ensure personnel who access Personal Data are subject to confidentiality obligations and receive adequate data protection training.
- Not transfer Personal Data outside the agreed jurisdiction, or to any third party, without QBA’s prior written authorization and appropriate safeguards.
- Assist QBA in responding to data subject requests (such as access, correction, or deletion requests) within agreed timeframes.
- Retain Personal Data only as long as necessary, and securely delete or return data upon termination of the contract as instructed by QBA.

5. Subcontracting

Suppliers shall not engage a subcontractor to process Personal Data on QBA’s behalf without QBA’s prior written consent, and shall ensure any approved subcontractor is bound by data protection obligations at least equivalent to those in this Policy.

6. Data Breach and Information Security Incidents

Suppliers shall inform QBA of any data breach or information security incident involving QBA or QBA’s client data within 48 hours of discovery, by notifying [Insert Security Incident Email]. Suppliers shall fully cooperate with QBA, including providing reasonable access to data processing facilities for investigation purposes.

Suppliers are expected to maintain adequate security controls to ensure the confidentiality, integrity, and availability of services provided to QBA and any QBA or client data processed or stored, and to support QBA's periodic security assessments.

7. Audits and Assurance

QBA reserves the right to request evidence of compliance, including security certifications, and to conduct audits or assessments of Supplier data protection practices, with prior intimation, either directly or through a nominated third party. Suppliers shall support such audits and provide corrective action plans within agreed timelines where findings are identified.

8. Non-Compliance and Policy Review

Failure to comply with this Policy may result in suspension of data processing activities, contractual remedies, or termination of the relationship, and may be reported to relevant supervisory authorities where required by law. This Policy will be reviewed periodically and Suppliers will be notified of material changes.

Document Code	Version	Effective Date	Prepared By	Approved By
QBA-POL-DP-01	1.0	January 2026	HR Head	Global CEO