DATA PROCESSING AGREEMENT (DPA)

Purpose — This Data Protection Addendum (“Addendum”) forms part of the agreement (“Agreement”) between **QLAMaster Ltd** (“QLAMaster” or **Processor**) and its customer (**Controller**) for the provision of services offered by QLAMaster.

Company details: QLAMaster Ltd, Company No. 16543970, 71–75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.

ICO registration: ZB939112.

This Addendum sets out the parties’ obligations under Article 28 UK GDPR / EU GDPR for the Processing of Personal Data.

1 Definitions

- Applicable Data Protection Law – UK GDPR, EU GDPR, the UK Data Protection Act 2018, and any national implementing laws.
- Data Subject, Personal Data, Processing, Supervisory Authority – have the meanings given in Applicable Data Protection Law.
- Sub-processor – any third party engaged by Processor to Process Personal Data on behalf of Controller.

2 Subject matter, duration & eligibility

Subject matter — Provision of QLAMaster’s online question-level analysis platform and related support services.

Duration — From the Effective Date of the Principal Agreement until deletion/return of Personal Data under Clause 9.

Nature & purpose — Hosting, storage, display, grading analytics, support, maintenance, and security monitoring.

Types of Personal Data — Names, school email addresses, class identifiers, assessment scores, login metadata, and billing/contact details for staff admins. Processor does not collect or store full payment card numbers or CVV.

Categories of Data Subjects — Teachers, school staff, pupils/students, and other authorised users.

Special category data — None intentionally; Controller will not transmit Article 9 data without prior written agreement.

Service eligibility — The Services are intended for use by schools and their authorised users aged 14 years and over. Student accounts are provisioned by the Controller (or by Processor at the Controller’s documented request); self-registration by students is not permitted. The Controller confirms it has a lawful basis to provide student Personal Data to the Processor and to permit student access.

3 Processor obligations

1. Process Personal Data only on the documented instructions of the Controller (including via the Principal Agreement and this Addendum).
2. Ensure persons authorised to process Personal Data are bound by confidentiality.
3. Implement and maintain the technical and organisational measures in Schedule A.
4. Assist the Controller, taking into account the nature of Processing, with Data Subject requests, DPIAs, and consultations with Supervisory Authorities.
5. Notify the Controller without undue delay (target: within 24 hours of awareness) of any Personal Data Breach, per Clause 8.
6. Make third-party audit and security reports reasonably available and allow on-site audits once per 12 months with 30 days' notice; additional audits are permitted following a Personal Data Breach affecting the Controller, a substantiated regulator request, or a material security incident.
7. Maintain Article 30(2) records of processing for Processor activities and provide summaries on request.
8. Given that Data Subjects include young people aged 14–17, apply age-appropriate safeguards, including least-privilege access, enhanced audit logging for access to student records, and staff screening proportionate to role.

4 Sub-processing

- The Controller authorises the Sub-processors listed in Schedule B (AWS UK/EU, Cloudflare EU, Stripe Payments UK Ltd).
- Processor will give at least 14 days' prior notice of new Sub-processors and allow the Controller to object on reasonable data-protection grounds.
- Notice of changes will be provided by email to the Controller's admin contact and via a published Sub-processors page.
- Processor will enter into Article 28-compliant written terms with each Sub-processor and remains fully liable for their acts and omissions.
- Payments: For cardholder data, Stripe acts as an independent controller. QLAMaster does not access or store payment card numbers or CVV.

5 International transfers

Processor will not transfer Personal Data outside the UK/EEA except where: (a) the destination benefits from an adequacy decision; or (b) transfers are made under the UK International Data Transfer Agreement, the EU Standard Contractual Clauses with the UK Addendum, or another valid transfer mechanism, together with any supplementary measures required to ensure an essentially equivalent level of protection.

6 Security & compliance documentation

Processor will maintain ISO 27001-aligned security policies (including a Data Security Policy and Breach Response Policy) and provide summaries on request.

7 Data Subject rights & cooperation

Taking into account the nature of Processing, Processor shall assist Controller by appropriate technical and organisational measures, insofar as possible, to respond to requests to exercise rights under Applicable Data Protection Law.

8 Personal Data Breach

Processor shall:

- notify the Controller at privacy@qlamaster.com without undue delay (target: within 24 hours of awareness);
- provide the information required by Article 33(3) GDPR as it becomes available, permitting staged notifications; and
- cooperate in good faith on containment, remediation, and any required regulatory and Data Subject notifications.

9 Return, deletion, and anonymisation

9.1 Return/export — Upon termination of the Agreement or on written request, Processor shall, at the Controller's choice, return all Personal Data or make it available for export in a commonly used format.

9.2 Deletion from active systems — Following (i) the Controller's confirmation that no further return/export is required or (ii) expiry of any agreed grace period for data export, Processor shall delete Personal Data from active systems within 30 days.

9.3 Backups — Encrypted backups are overwritten in the ordinary course of rotation (typically within 35–90 days).

9.4 Post-termination retention & anonymisation — Unless the Controller instructs earlier deletion, Processor may retain a minimal subset of Personal Data strictly necessary for security, audit, and legal accountability. Such data will be irreversibly anonymised no later than 24 months after the end of the subscription (the "Anonymisation Date").

9.5 Definition — "Anonymisation" means an irreversible process after which data cannot reasonably be re-identified by the Processor, the Controller, or third parties, taking account of available means and the context of Processing.

9.6 Certification — On request, Processor will provide written confirmation of deletion and/or anonymisation.

10 Liability & indemnity

Each party's liability under this Addendum is subject to the limitations and exclusions in the Principal Agreement. The Processor shall indemnify the Controller against third-party claims arising from the Processor's breach of this Addendum or Applicable Data Protection Law, to the extent permitted by law, excluding losses caused by the Controller's instructions or omissions and in all cases subject to the liability caps in the Principal Agreement.

11 Miscellaneous

- In case of conflict, this Addendum prevails over the Principal Agreement regarding Personal Data Processing.
- Governing law and venue: as set out in the Principal Agreement (default: England & Wales).
- Hosting: QLAMaster's production services run on AWS UK/EU regions.

Schedule A — Technical & organisational measures (Article 32)

Encryption

- AES-256 encryption at rest; TLS 1.2+ in transit.

Identity, access & authentication

- MFA on all admin accounts; role-based access control with least-privilege; quarterly access reviews.
- Passwords stored using strong, industry-standard hashing.
- Optional MFA support for school tenants where available.

Systems hardening & change control

- Segregated environments (prod/dev).
- Patch management on a regular cadence; change control with rollback plans.

Monitoring, logging & detection

- Centralised log collection

Backups & resilience

- Encrypted rolling backups in AWS UK region

Testing & assurance

- Annual CREST-accredited penetration testing (or equivalent) and remediation tracking.
- Secure SDLC practices including dependency management and vulnerability scanning.

Staff & organisation

- Security and privacy training for relevant staff; background screening proportionate to role.
- Vendor and sub-processor risk management.

Data minimisation & privacy by design

- Support for use of pseudonymous student IDs where feasible; collect only data necessary for QLA functionality.

- Procedures for secure deletion/disposal.

Physical & cloud infrastructure

- Physical security controls inherited from AWS (data centre access controls, environmental safeguards).

Schedule B — Approved Sub-processors

Name	Service	Location	Role	Safeguard
Amazon Web Services (AWS) UK Ltd	Cloud hosting & encrypted storage	London / Dublin	Processor	Intra-EEA/UK processing; SCCs/UK Addendum if applicable
Cloudflare, Inc.	Edge security & traffic routing (EU PoPs by default)	EU PoPs	Processor	EU SCCs + UK Addendum (and supplementary measures as required)
Stripe Payments UK Ltd	Secure payment processing & tokenisation	EU data centre	Independent controller for card data	EU SCCs + UK Addendum (as applicable)

Change notifications: Processor will give ≥14 days' prior notice of any new Sub-processor by email to the Controller's admin contact and on the Sub-processors webpage.

Schedule C — Data retention & deletion

Data class	Retention	Disposition
Student & staff profile data (names, emails, class IDs)	Subscription term; deleted from active systems within 30 days of termination; minimal subset retained for security/audit until the Anonymisation Date	Anonymised ≤ 24 months post-subscription end; earlier on Controller instruction
Assessment data (scores, QLA responses, reports)	Same as above	QLA outputs may be preserved only in fully anonymised form after the Anonymisation Date
Operational logs	6 years	Secure deletion on expiry

Security/audit logs	6 years	Secure deletion on expiry
Backups	Rolling encrypted backups, up to 35 days	Overwritten in normal rotation
Billing records for staff admins	Per legal/tax requirements (typically 6 years in the UK)	Secure deletion on expiry