Quotation Bank: Exam Revision

DATA PROCESSING AGREEMENT (DPA)

_____

This Data Processing Agreement ("DPA") forms part of the Services Agreement or Terms of Service between the Customer (the "Data Controller") and Esse Publishing Limited (the "Data Processor").

1. Definitions

For the purposes of this DPA:

- **"Data Protection Laws"** means all applicable data protection and privacy legislation in force from time to time in the UK, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- **"Personal Data"**, **"Data Subject"**, **"Data Controller"**, **"Data Processor"**, and **"Processing"** shall have the meanings given to them in the Data Protection Laws.

2. Scope and Roles

2.1. The parties acknowledge that for the purposes of the Data Protection Laws, the Customer is the Data Controller and Esse Publishing Limited is the Data Processor.

2.2. The Processor shall only process Personal Data on the documented instructions of the Controller, unless required to do so by UK law.

3. Details of Processing

Subject Matter: The processing of Personal Data to provide educational, assessment and e-learning services via Esse Publishing Limited.

Duration: For the duration of the Principal Agreement and thereafter only for so long as required in accordance with Section 8.

Nature and Purpose: To create and manage user accounts; authenticate users; deliver educational content and quizzes; process student responses; manage classes, schools, and administrative access; and maintain platform security, fraud prevention, diagnostics, and service reliability.

Types of Personal Data: email addresses, authentication and login data, IP addresses and device or browser metadata, school and class affiliation data, user-generated content including quiz responses, and other account or service data linked to an identifiable user.

Categories of Data Subjects: Students, teachers, school administrators, and other authorised users of the platform.

4. Data Location and International Transfers

4.1. Primary Hosting of Personal Data: The Processor hosts and stores the Controller's core platform Personal Data primarily within United Kingdom infrastructure for core application and database operations.

4.2. International Transfers of Personal Data: Notwithstanding Section 4.1, the Processor may transfer limited Personal Data outside the United Kingdom where necessary to provide the services through approved sub-processors listed in Section 9.3, including for bot protection, file delivery, error monitoring, diagnostics, and related operational support. Any such transfers shall be limited to the data necessary for the relevant purpose and made subject to appropriate safeguards under applicable Data Protection Laws.

5. Technical and Organisational Measures (TOMs)

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

Encryption: All Personal Data shall be encrypted both in transit and at rest.

Access Controls: Strict Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) are enforced for all internal staff accessing systems containing Personal Data. The principle of least privilege is applied.

Firewalls and Monitoring: Implementation of robust firewalls, intrusion detection systems, and continuous network monitoring to restrict unauthorised access.

6. Personal Data Breaches

6.1. In the event of a Personal Data breach affecting the Controller's data, the Processor shall notify the Controller without undue delay, and in any event within 72 hours of becoming aware of the breach.

6.2. The Processor will provide the Controller with sufficient information to allow the Controller to meet any obligations to report to the Information Commissioner's Office (ICO) or inform Data Subjects.

7. Data Subject Rights (DSARs)

7.1. Data Retrieval: The Processor's systems are structured to ensure that Personal Data is easily accessible to the Controller. The Processor provides the Controller with the necessary administrative functionality and data export tools to easily and promptly retrieve any Personal Data required to fulfil a Data Subject Access Request (DSAR).

7.2. Direct Requests: If the Processor receives a DSAR, a request for erasure, or any other data protection request directly from a Data Subject (e.g., a student, teacher, or parent), the Processor will not respond to the request directly. The Processor will notify the Controller immediately (and in any event within 48 hours of receipt) and await the Controller's instructions.

7.3. Assistance: The Processor shall provide all reasonable and timely assistance to the Controller to enable the Controller to respond to any such requests within statutory timeframes.

8. Data Retention and Deletion

8.1. Default Retention Period: Unless otherwise instructed by the Controller, the Processor shall retain the Controller's Personal Data for a period of two (2) years following the termination or expiry of the Principal Agreement. At the end of this two-year period, all Personal Data will be securely and permanently deleted from active systems.

8.2. Controller's Control and Right to Delete: The Controller retains full control over their data at all times. The Controller may instruct the Processor to delete data attached to specific individual accounts, or request the deletion of all their data, at any time during the active relationship or after its termination. The Processor will execute this permanent deletion from live systems promptly upon receiving the Controller's written request.

8.3. Backups and Archives: Upon a triggered deletion, Personal Data is permanently deleted from live, active databases. Where Personal Data remains in secure automated backups or disaster recovery archives, it will be put beyond use and permanently overwritten in accordance with the Processor's standard backup retention period.

9. Sub-processors

9.1. The Controller provides specific written authorisation for the Processor to engage the sub-processors listed in Section 9.3 to deliver the services.

9.2. The Processor shall enter into a written agreement with any sub-processor imposing data protection obligations no less protective than those set out in this DPA.

9.3. Approved Sub-processors:

The Processor currently engages the following sub-processors:

Sub-processor	Purpose of Processing	Data Type Processed
Supabase	Authentication, database, user/session management, app records	Email, password, user ID, auth tokens/sessions, student/school associations, quotation/bookmark/subscription records, Expo push token, deletion request type
Expo	Push notification, token registration and push delivery	Expo push token, notification permission state, notification payload/body, device/app project info; IP unspecified
Sentry	Crash and Error Monitoring	IP address, device/runtime info, request URLs/query strings, crash/error telemetry; logged-in user data unspecified
PostHog	Product analytics and session replay	User ID, email, account created_at, platform, subscription status, analytics events, session replay data; GeoIP disabled; precise event schema unspecified

9.4. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller the opportunity to object to such changes. If the Controller has a reasonable, data-protection-related objection that cannot be resolved, they may terminate the applicable services.