Spelling Mastery — School Compliance Pack

Executive Security and Privacy Overview

Document owner: [Company Name] Version: 1.0 Last updated: [YYYY-MM-DD]

1. Purpose

This document summarizes the privacy, security, and compliance position of Spelling Mastery for school procurement and governance review.

2. Service Scope

Spelling Mastery is a school-focused spelling practice platform. Core processing activities:

- Student account administration (school-managed)
- Spelling practice and progress tracking
- Teacher/admin reporting
- Optional text-to-speech for pronunciation support

3. Data Protection Model

- School/Trust: Data Controller
- Spelling Mastery: Data Processor
- Lawful basis: Defined by the school as controller (typically public task, legal obligation, or consent where required)

4. Personal Data Categories

Typical categories:

- Identity data: name, username, class/group
- Account data: role, school affiliation, login metadata
- Learning data: words attempted, correctness, timestamps
- Security data: audit and authentication events

Special category data is not intentionally required for normal service use.

5. Core Security Controls

- Encryption in transit (TLS)

- Encryption at rest via managed cloud providers
- Role-based access controls
- Tenant separation controls
- Input validation and secure error handling
- Audit logging for privileged operations
- Operational monitoring and incident handling process

6. Compliance Artifacts Available

This pack includes:

- Data Processing Agreement template
- Retention and deletion policy
- Data subject rights procedure
- Incident response and breach notification process
- TOMs statement
- Subprocessor and international transfer register
- ROPA
- DPIA template
- BCDR policy
- Access control policy

7. Security and Privacy Contacts

Privacy contact: [privacy@your-domain] DPO/contact point: [dpo@your-domain] Security contact: [security@your-domain]

8. Commitments

Spelling Mastery commits to:

- Processing personal data only on documented controller instructions
- Supporting controller obligations under UK GDPR/GDPR
- Maintaining proportionate technical and organizational safeguards
- Prompt incident notification in accordance with contractual terms and law

9. Legal Note

This document is informational and does not replace legal advice. Controller-specific requirements should be finalized in the signed contract and DPA.