Spelling Mastery — School Compliance Pack

Technical and Organisational Measures (TOMs)

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

1. Security Governance

- Defined security ownership and escalation contacts
- Policy framework for access, incident, retention, and change control
- Periodic risk review and remediation tracking

2. Access Control

- Role-based access aligned to least privilege
- Admin access restricted to authorized personnel
- Access review and prompt deprovisioning for role changes/leavers

3. Authentication and Session Security

- Strong authentication controls for privileged users
- Session/token validation on protected API routes
- Brute-force protection/rate limiting on login workflows

4. Data Segregation

- Tenant (school) scoping controls to prevent cross-tenant access
- Authorization checks at application and data layer

5. Encryption

- Encryption in transit using TLS
- Encryption at rest via managed cloud platform controls
- Secure key/secret handling in environment configuration

6. Secure Development Practices

- Input validation and output handling controls
- Structured error handling to avoid sensitive leakage

- Change management with code review before deployment

7. Logging and Monitoring

- Audit logs for sensitive administrative actions
- Security event logging and alerting for anomalies
- Log retention aligned to documented policy

8. Vulnerability Management

- Dependency and configuration reviews
- Prioritized remediation based on risk severity
- Retesting for high-risk findings

9. Backup and Recovery

- Automated backups
- Defined recovery objectives and restoration procedures
- Periodic restoration testing

10. Supplier Management

- Subprocessor due diligence and contractual data protection terms
- Transfer mechanism controls for international data flows