Spelling Mastery — School Compliance Pack

Incident Response and Breach Notification Procedure

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

1. Purpose

Defines how security incidents are triaged, contained, investigated, and communicated to school controllers.

2. Incident Severity Model

Severity	Description	Target Initial Response
Critical	Confirmed high-impact data compromise or service-wide outage	Immediate, 24/7
High	Likely compromise or major degradation	Within [4] hours
Medium	Limited impact event	Within [1] business day
Low	Minor issue/no confirmed impact	Planned remediation

3. Response Lifecycle

1. Detect and register incident.
2. Triage and classify severity.
3. Contain affected systems/accounts.
4. Eradicate root cause and recover service.
5. Perform forensic and impact assessment.
6. Notify controllers as required.
7. Complete post-incident review and corrective actions.

4. Breach Notification to Schools

Processor notifies affected controller without undue delay after becoming aware of a personal data breach. Notification includes known details:

- incident summary and timeline
- data categories and estimated scope
- likely consequences

- mitigation steps taken
- recommended controller actions
- contact point for follow-up

5. Regulatory Support

Processor supports controller with information needed for regulatory reporting (for example ICO reporting window under UK GDPR), while controller remains responsible for filing obligations.

6. Evidence and Record Keeping

Incident records include:

- detection source
- actions and timestamps
- decision log
- communications sent
- lessons learned and remediation owners

7. Testing

Tabletop or simulation exercises should be run at least annually and after major architecture changes.