

Security Questionnaire Responses (School Procurement)

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

1. Organization and Governance

Q: Do you have a named privacy/security contact? A: Yes. Contacts are documented in the executive overview and contract pack.

Q: Do you maintain data protection and security policies? A: Yes. This pack includes retention, incident, TOMs, and access control policies.

2. Data Protection

Q: Are you a controller or processor for school data? A: Processor. The school/trust is the controller.

Q: Do you provide a DPA? A: Yes. See 02-Data-Processing-Agreement-DPA-Template.md.

Q: Do you support data subject rights requests? A: Yes. See 04-Data-Subject-Rights-Procedure-UK-GDPR.md.

3. Security Controls

Q: Is data encrypted in transit and at rest? A: Yes, via TLS in transit and cloud-provider encryption at rest.

Q: Is access role-based and least-privilege? A: Yes. See 12-Access-Control-and-Identity-Management-Policy.md.

Q: Are admin/security events logged? A: Yes. Administrative actions are logged for audit and investigation support.

4. Incident Management

Q: Do you have an incident response process? A: Yes. See 05-Incident-Response-and-Breach-Notification-Procedure.md.

Q: Will schools be notified of personal data breaches? A: Yes, without undue delay after awareness, with available details.

5. Resilience

Q: Do you maintain backup and recovery processes? A: Yes. See 11-Business-Continuity-and-Disaster-Recovery-BCDR.md.

Q: Do you test recovery? A: Recovery procedures are tested periodically and after significant platform changes.

6. Supply Chain and Transfers

Q: Do you use subprocessors? A: Yes, listed in 07-Subprocessor-and-International-Transfers-Register.md.

Q: How are international transfers handled? A: Through appropriate legal mechanisms and supplementary safeguards where required.

7. Compliance and Assurance

Q: Can you support school DPIA completion? A: Yes. See 09-DPIA-Template-School-Use.md.

Q: Can you provide evidence updates during contract term? A: Yes, subject to confidentiality and reasonable audit terms.