

Data processing agreement

Between the school, trust or other organisation using SchoolProof (the "Controller") and Alacria Limited, company number 17395232, registered office 2 Reid Court, Little Sutton, Ellesmere Port, Wirral, CH66 1SB (the "Processor"). This agreement forms part of the SchoolProof terms of service and applies from the moment the Controller creates a SchoolProof account.

1. What this covers

The Processor provides the SchoolProof platform: a readiness check, compliance audit, procedure register, staff sign-offs, drill log, evidence pack and, where switched on, visitor and staff sign-in. In doing so it processes personal data on the Controller's behalf and on the Controller's documented instructions, which are the terms of service, the settings the Controller chooses in the platform and any written instruction from the Controller.

2. The data

Data subjects: the Controller's staff, governors and volunteers who use or are named in the platform; visitors and contractors signed in at the Controller's premises; pupils only where the Controller chooses to name them in free-text fields (for example individual emergency arrangements).

Categories: names, work email addresses, job roles, sign-in and sign-out times, organisation, vehicle registration where the Controller asks for it, answers to audit questions, uploaded procedure documents, and records of who acknowledged, reviewed or exercised a procedure.

Duration: for as long as the Controller has a SchoolProof account, subject to the retention periods in section 7.

3. The Processor's obligations

The Processor will: process the data only on the Controller's documented instructions, and tell the Controller if it believes an instruction breaks data protection law; ensure everyone it authorises to process the data is bound by confidentiality; put in place the technical and organisational measures in section 5; help the Controller respond to requests from data subjects, and to meet its obligations on security, breach notification and impact assessments, taking account of the nature of the processing; delete or return the data at the end of the service as set out in section 7; and make available the information needed to demonstrate compliance, and allow for and contribute to audits and inspections by the Controller or an auditor it mandates, on reasonable notice.

4. Sub-processors

The Controller gives general authorisation for the Processor to use the sub-processors below. The Processor will give at least 30 days' notice on /your-data before adding or replacing one, and the Controller may object in writing; if the objection cannot be resolved, the Controller may terminate.

Microsoft Azure (Microsoft Ireland Operations Ltd): hosting, database, file storage and application monitoring, in the UK South region.

Microsoft Azure Communication Services: sending the platform's transactional email (invitations, reminders, reports, invoices).

No other organisation receives personal data. No data is sold or used for advertising.

5. Security

Data is held in Microsoft Azure's UK South region, encrypted in transit (TLS) and at rest. Each school's data is isolated at the database level so one school can never see another's. Access to production systems is limited to

named Processor staff with multi-factor authentication. Uploaded documents are stored in Azure Blob Storage, not on web servers. The platform keeps an append-only audit trail of meaningful actions. Automated daily backups are retained by Azure Database for PostgreSQL for at least seven days. The Processor sets no tracking cookies and uses no third-party analytics.

6. Personal data breaches

The Processor will notify the Controller without undue delay, and in any case within 24 hours of becoming aware of a personal data breach affecting the Controller's data, with the information the Controller needs to meet its own 72-hour obligation to the ICO, and will co-operate in containing and remedying the breach.

7. Retention, return and deletion

Free readiness check data with no account: deleted 24 months after last activity. Visitor sign-in records: deleted after the retention period the Controller sets (12 months by default). Staff sign-in records: deleted after 31 days. Account, audit, procedure and evidence data: kept for the life of the account. When the account ends, the Controller may export its evidence pack and documents at any time before termination; the Processor deletes the Controller's data within 30 days of termination unless the Controller asks in writing for earlier deletion or a copy first. Backups expire on their normal cycle.

8. International transfers

The Processor does not transfer the Controller's personal data outside the United Kingdom. Microsoft may provide support from outside the UK under its own UK GDPR-compliant terms; no Controller data is moved to do so.

9. Liability and law

Each party is responsible for its own compliance with UK GDPR and the Data Protection Act 2018. Liability is as set out in the SchoolProof terms of service. This agreement is governed by the law of England and Wales.

Questions or a supplier questionnaire: hello@schoolproof.co.uk. This agreement is provided for the Controller's records and does not need to be signed to take effect; a signed copy is available on request.