

Data Processing Agreement

Version 1.0 — Effective Date: [Insert Date]

This Data Processing Agreement (“DPA”) forms part of the Master Services Agreement between SchoolCentralX (operated by Volume Media Limited, registered in England) and the subscribing educational institution (“School”, “Controller”).

1. Definitions

“Controller”: The School that determines the purposes and means of processing personal data.

“Processor”: SchoolCentralX (Volume Media Limited), processing personal data on behalf of the Controller.

“Data Subject”: An identified or identifiable natural person whose personal data is processed.

“Personal Data”: Any information relating to a Data Subject as defined by the UK GDPR.

“Sub-processor”: A third party engaged by the Processor to process Personal Data on behalf of the Controller.

“Applicable Data Protection Law”: The UK GDPR, Data Protection Act 2018, and any successor legislation.

2. Scope and Purpose of Processing

The Processor shall process Personal Data solely for the purpose of providing the SchoolCentralX platform services, including:

- Facilitating communication between the School and parents/guardians
- Managing student records, attendance, behaviour tracking, and homework
- Providing analytics and engagement insights to school administrators
- Storing and transmitting media uploaded by the School

Processing shall continue for the duration of the subscription and any post-termination retention period.

3. Categories of Data Subjects and Personal Data

Data Subjects: Students, parents/guardians, school staff and administrators.

Personal Data categories:

- Names, email addresses, contact details

- Student identifiers and class/group assignments
- Attendance records, behaviour notes, homework submissions
- Photos and media uploaded by the School
- Communication logs (messages between school and parents)
- Technical data (IP addresses, device information, usage analytics)

4. Obligations of the Processor

The Processor shall:

- a) Process Personal Data only on documented instructions from the Controller, unless required by law.
- b) Ensure persons authorised to process Personal Data are bound by confidentiality obligations.
- c) Implement appropriate technical and organisational measures to ensure security appropriate to the risk (see Annex A of the Privacy Policy).
- d) Not engage another processor without prior written authorisation of the Controller.
- e) Assist the Controller in responding to Data Subject requests within 30 days.
- f) Assist the Controller in ensuring compliance with security, breach notification, DPIAs, and prior consultation obligations.
- g) At the Controller's choice, delete or return all Personal Data upon termination.
- h) Make available all information necessary to demonstrate compliance and allow for audits.

5. Obligations of the Controller

The Controller shall:

- a) Ensure it has a lawful basis for processing Personal Data and for instructing the Processor.
- b) Provide clear and documented processing instructions.
- c) Ensure Data Subjects are informed about the processing in accordance with Applicable Data Protection Law.
- d) Respond to Data Subject requests, with assistance from the Processor as needed.

6. Sub-processors

The Processor currently uses the following categories of sub-processors:

- Cloud infrastructure providers (hosting and database services)
- Payment processors (billing and subscription management)
- Analytics providers (anonymised usage data only)

- Email delivery services (transactional notifications)

A current list of sub-processors is available on request. The Controller will be notified at least 30 days before any new sub-processor is engaged.

7. International Data Transfers

Where Personal Data is transferred outside the UK or EEA, the Processor shall ensure appropriate safeguards including:

- UK International Data Transfer Agreement (IDTA) or EU Standard Contractual Clauses (SCCs)
- Transfer Impact Assessments where required
- Processing only in jurisdictions with adequate data protection standards where possible

8. Security Measures

The Processor implements the following measures (detailed in Annex A of the Privacy Policy):

- TLS 1.3 encryption in transit; AES-256 encryption at rest
- Role-based access controls with multi-factor authentication for administrators
- Comprehensive logging and monitoring of all data access
- Secure development lifecycle with code reviews and dependency scanning
- Quarterly penetration testing by an independent security firm
- Encrypted back-ups retained for a maximum of 90 days
- Employee training and confidentiality agreements

9. Data Breach Notification

In the event of a Personal Data breach, the Processor shall:

- a) Notify the Controller without undue delay and within 24 hours of becoming aware of the breach.
- b) Provide sufficient information for the Controller to notify the supervisory authority within 72 hours.
- c) Co-operate with the Controller in investigating and mitigating the breach.
- d) Document the breach, its effects, and the remedial action taken.

10. Data Retention and Deletion

Personal Data shall be retained per the Data Retention and Deletion Policy in the SchoolCentralX Privacy Policy. Key periods:

- School account data: active subscription + 12 months

- Parent accounts: active link + 6 months
- Student records: controlled by the School
- Chat/messages: 12 months (anonymised then purged)
- System logs: 180 days (auto-purged)

Upon termination, all data is deleted within 30 days; back-ups within 90 days. A certificate of deletion is available on request.

11. Audit Rights

The Controller may audit the Processor's compliance with this DPA, subject to reasonable notice and during business hours. The Processor shall co-operate fully.

12. Liability and Indemnification

Each party's liability under this DPA shall be subject to the limitations in the Master Services Agreement. Each party shall indemnify the other against costs, claims, or damages arising from a breach of this DPA.

13. Term and Termination

This DPA commences on the effective date and continues for the duration of the Master Services Agreement. It terminates automatically upon expiry or termination of the Master Services Agreement, subject to surviving data deletion obligations.

14. Governing Law

This DPA shall be governed by the laws of England and Wales. Disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

15. Signatures

FOR THE CONTROLLER (School)

Name: _____

Title: _____

Organisation: _____

Date: _____

Signature: _____

FOR THE PROCESSOR (SchoolCentralX)

Name: _____

Title: _____

Organisation: Volume Media Limited

Date: _____

Signature: _____

Contact for DPA queries: dpo@schoolcentralx.com