



Data Processing Agreement

Version 1.3 | 19 October 2026

Terms for processing school-controlled personal data

Status	Current Version 1.3 19 October 2026
--------	---

This Data Processing Agreement forms part of the agreement under which Fullscoped provides its school self-evaluation platform. It applies where Fullscoped processes personal data on behalf of a school or other education organisation.

Document completion

Complete the customer details before signature. A school should review this agreement alongside its own data protection assessment and procurement requirements.

Privacy contact: privacy@fullscoped.co.uk

Security incident contact: security@fullscoped.co.uk

Website: www.fullscoped.co.uk | Application: app.fullscoped.co.uk

Principal database: Supabase on AWS eu-west-2, London, United Kingdom. Application delivery: Vercel and Cloudflare global networks. Transactional email: Resend. Production database backups run daily with seven-day retention.

Parties

Item	Details
Controller	The school or education organisation identified in the Order Form or other applicable written agreement (Customer).
Processor	Fullscoped Ltd, company number 17473090, registered office 71–75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom (Fullscoped).
Privacy contact	privacy@fullscoped.co.uk
Security incident contact	security@fullscoped.co.uk
Effective date	The date the Customer first receives access to the service or the date of signature, whichever is earlier.



1 Status and scope

1.1 This Data Processing Agreement (DPA) forms part of the agreement between the Customer and Fullscoped for use of the Fullscoped service (Main Agreement). If there is a conflict about personal data processing, this DPA takes priority over the Main Agreement.

1.2 The Customer is the controller and Fullscoped is the processor for Customer Personal Data, except where the parties' actual processing roles require otherwise under Data Protection Law.

1.3 Fullscoped is an independent controller for personal data it uses for its own account administration, billing, security, legal compliance and business communications, as described in the Fullscoped Privacy Notice.

2 Definitions

In this DPA, Customer Personal Data means personal data processed by Fullscoped on behalf of the Customer through the service. Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and other applicable UK data protection law, each as amended. The terms controller, processor, personal data, processing, personal data breach and data subject have the meanings given by Data Protection Law.

3 Processing instructions

3.1 Fullscoped will process Customer Personal Data only on the Customer's documented instructions, including the instructions set out in the Main Agreement, this DPA and the Customer's authorised use of the service, unless UK law requires other processing.

3.2 If UK law requires Fullscoped to process Customer Personal Data other than on the Customer's instructions, Fullscoped will notify the Customer before processing unless the law prohibits that notification for important grounds of public interest.

3.3 Fullscoped will promptly inform the Customer if, in its reasonable opinion, an instruction infringes Data Protection Law. Fullscoped may suspend the affected processing while the parties resolve the issue.

3.4 The Customer is responsible for the lawfulness, fairness and transparency of its processing; the accuracy and quality of Customer Personal Data; its instructions; and ensuring authorised users comply with the service rules.



4 Details of processing

Item	Description
Subject matter	Providing and supporting a hosted school self-evaluation, review and improvement-planning platform.
Duration	For the term of the Main Agreement. Customer Personal Data is normally deleted within 30 days after termination, subject to the Customer's export choice, legal requirements and any applicable backup-expiry period.
Nature and purpose	Hosting, storing, organising, retrieving, displaying, transmitting at the Customer's request, backing up, securing, supporting and deleting Customer Personal Data so authorised users can use the service.
Data subjects	Primarily authorised school staff, governors, trustees and other organisation representatives. The service is not designed to store identifiable pupil data.
Personal-data types	Names, work email addresses, roles, access permissions, audit and usage records, support information, and any incidental personal data included by authorised users in review content.
Special-category data	Not intended or permitted. Users are instructed not to enter medical information, safeguarding case details or other identifiable sensitive personal data.
Frequency	Continuous or intermittent while authorised users use the service.
Customer instructions	The Main Agreement, configured permissions, actions of authorised users and written instructions agreed by the parties.

5 Confidentiality and personnel

5.1 Fullscoped will ensure that people authorised to process Customer Personal Data are subject to an appropriate duty of confidentiality and receive relevant data protection and security guidance.

5.2 Fullscoped will limit access to people who need it to provide, secure or support the service.

6 Security

6.1 Taking account of the state of the art, implementation costs, and the nature, scope, context and purposes of processing, Fullscoped will maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

6.2 Measures will include, as appropriate to risk:

- access controls and role-based permissions;
- authentication controls and secure password handling;
- encryption in transit and supplier-supported encryption at rest;
- logging, monitoring and investigation of relevant security events;



secure development, change control and dependency management;

backup, recovery and service-continuity arrangements;

supplier due diligence and contractual controls; and

periodic review of security measures and access.

6.3 Fullscoped may update its measures as technology and risks evolve, provided the overall protection is not materially reduced.

7 Personal data breaches

7.1 Fullscoped will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

7.2 The notification will include, so far as information is available, the nature of the breach; likely consequences; categories and approximate numbers of affected data subjects and records; measures taken or proposed; and a contact for further information. Fullscoped may provide information in phases as the investigation develops.

7.3 Fullscoped will take reasonable steps to contain, investigate and mitigate the breach and will cooperate with the Customer. The Customer remains responsible for deciding whether to notify the ICO or affected individuals.

8 Data subject requests

8.1 Taking account of the nature of the processing, Fullscoped will provide reasonable technical and organisational assistance to help the Customer respond to requests to exercise data protection rights.

8.2 If Fullscoped receives a request relating to Customer Personal Data, it will not respond substantively except on the Customer's instructions or where legally required. It will promptly direct the request to the Customer where practicable.

9 Compliance assistance

Taking account of the nature of processing and information available to it, Fullscoped will provide reasonable assistance with the Customer's obligations concerning security, breach management, data protection impact assessments and prior consultation with the ICO. Assistance beyond normal service operation may be subject to reasonable agreed charges where the need was not caused by Fullscoped's breach of this DPA.

10 Subprocessors

10.1 The Customer gives Fullscoped general written authorisation to use subprocessors needed to provide the service. The authorised subprocessors at the effective date are listed in Schedule 2.

10.2 Fullscoped will provide notice of an intended new or replacement subprocessor before that subprocessor begins processing Customer Personal Data. The Customer may object on reasonable data-protection grounds within 14 days of notice. The parties will work in good faith to resolve the objection. If no reasonable solution is available, the Customer may terminate the affected service without penalty.

10.3 Fullscoped will enter into a written agreement with each subprocessor imposing data protection obligations that provide materially equivalent protection to this DPA. Fullscoped remains responsible to the Customer for its subprocessors' performance of those obligations.



11 International transfers

11.1 Fullscoped will not make a restricted transfer of Customer Personal Data outside the United Kingdom unless it complies with Data Protection Law and the transfer is covered by an applicable safeguard.

11.2 Safeguards may include UK adequacy regulations, the UK International Data Transfer Agreement, or the UK Addendum to approved standard contractual clauses, together with any required transfer risk assessment and supplementary measures.

11.3 Fullscoped will provide reasonable information about applicable transfer safeguards on request, subject to confidentiality and security restrictions.

12 Return and deletion

12.1 On expiry or termination, and at the Customer's choice, Fullscoped will delete or return Customer Personal Data and delete remaining copies unless UK law requires retention. The Customer must request an available export before account closure where it wishes to retain the data.

12.2 Where backups apply, data may remain temporarily in protected backups until overwritten through the ordinary backup cycle. During that period it will remain protected and will not be restored except for disaster recovery, security investigation or legal necessity. Fullscoped will make the applicable backup-expiry period available to the Customer.

12.3 Fullscoped may retain limited evidence necessary to demonstrate compliance or establish, exercise or defend legal claims, where permitted by law.

13 Information and audits

13.1 Fullscoped will make available information reasonably necessary to demonstrate compliance with Article 28 of the UK GDPR, including relevant policies, summaries, questionnaires and independent assurance when available.

13.2 If that information is insufficient, the Customer may request an audit. Audits must be proportionate, normally no more than once each year, conducted on reasonable written notice during business hours, and designed to avoid unnecessary disruption and risks to other customers' confidentiality and security.

13.3 The Customer will bear reasonable audit costs unless the audit identifies a material breach by Fullscoped. Nothing requires Fullscoped to disclose information that would compromise another customer, security controls or legally protected material.

14 Customer responsibilities

The Customer will:

use the service only for lawful school self-evaluation and improvement purposes;

ensure it has a lawful basis and provides required privacy information;

configure and review user access appropriately;

keep credentials secure and promptly remove access that is no longer required;

avoid entering pupil names, safeguarding case details, medical information or other identifiable sensitive personal data;

refer to secure school systems instead of reproducing individual pupil or sensitive records; and

notify Fullscoped promptly of suspected unauthorised access or security concerns.



15 Liability and general terms

15.1 Liability under this DPA is subject to the exclusions and limits in the Main Agreement, except to the extent those exclusions or limits are prohibited by law.

15.2 No failure or delay in exercising a right under this DPA waives that right. If a provision is unenforceable, it will be adjusted to the minimum extent necessary and the remaining provisions will continue.

15.3 This DPA is governed by the law and jurisdiction specified in the Main Agreement. If the Main Agreement does not specify them, the laws of England and Wales apply and the courts of England and Wales have exclusive jurisdiction.

Schedule 1 Processing details

The processing details in clause 4 form Schedule 1. The Customer may document additional lawful instructions in the Order Form or another written agreement, provided they are consistent with the service and this DPA.

Schedule 2 Authorised subprocessors

Item	Service and processing
Supabase	Database, authentication and application backend. The primary database is hosted in London, United Kingdom (AWS eu-west-2). Supplier support and operational processing may involve restricted transfers covered by the supplier's applicable contractual safeguards.
Vercel	Hosting and global delivery of the static Fullscoped application interface. Fullscoped does not use Vercel as persistent storage for school workspace records. Restricted transfers are covered by the supplier's applicable contractual safeguards.
Resend	Transactional email delivery for invitations, password resets and service communications. Resend is a United States provider. Applicable transfers are covered by its data processing terms, including recognised transfer mechanisms such as the UK Extension to the EU-US Data Privacy Framework where applicable and contractual safeguards.
Cloudflare	DNS, web security, public website hosting and administration API processing. Cloudflare Workers operate through a global network. The main school workspace database remains in Supabase London.
Zoho Mail	Business email and customer correspondence using Zoho's European data centre service.

OpenAI OpCo, LLC (optional AI only): API processing of selected school-level text, with international processing and retention as detailed in Schedule 4. Not activated for the Customer without the required authorisation.

Schedule 3 Security summary

The security measures in clause 6 form the initial security summary. Fullscoped maintains an operational record of hosting locations, supplier terms, backup arrangements, retention settings, incident contacts, access reviews and recovery testing. The production Supabase project uses automated daily backups with seven-day retention.



Schedule 4 Optional AI processing instructions

This schedule applies only after the Customer's authorised representative accepts the versioned AI arrangements and Fullscoped activates an AI period. Acceptance is an instruction to use the optional subprocessor for the selected task, not pupil or staff consent. The existing notice and objection procedure in clause 10.2 continues to apply before a new subprocessor processes Customer Personal Data.

Subject matter and purpose: drafting proposed school-level SEF/SDP wording and planning improvements, and comparing selected review snapshots for governor reports. Nature: transmitting the selected extracts and user update to the OpenAI API, processing the returned draft and presenting it for human review. Frequency: individual requests by authorised adult administrators or editors; no routine background AI processing. Data types: school-level evaluation and planning text, aggregate results and incidental personal data in free text. Identifiable pupil information, individual cases, special-category and criminal-offence information are not intended or permitted.

Additional optional subprocessor: OpenAI OpCo, LLC, United States, for API inference and associated service security, with its published affiliates and subprocessors. Processing may occur outside the UK. Before activation, Fullscoped must put its applicable OpenAI DPA, UK transfer safeguards and any required assessment in place. OpenAI's DPA includes standard contractual clauses as amended by the UK Addendum for UK data. Fullscoped remains responsible under clause 10.3.

Fullscoped submits generation requests with store=false. API data is not used for model training by default. This is not a Zero Data Retention arrangement: standard abuse-monitoring logs may contain inputs and outputs, normally retained up to 30 days, with legal/safety exceptions; temporary prompt caching may also apply. Approved wording becomes normal workspace content. The usage ledger holds metadata, not prompts or outputs. Provider retention, assistance and deletion operate under its DPA and the AI arrangements. Disabling AI stops future generation without deleting approved workspace content. Fullscoped will assist with relevant requests under clauses 8, 9 and 12.

The school must assess its proposed use, involve its DPO/adviser where appropriate, provide required privacy information and complete a DPIA where processing is likely to result in high risk. No AI decision about an individual pupil or staff member is authorised.

Signatures

For the Customer	For Fullscoped Ltd
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date: