



Assistant SENDCo

Data Processing Addendum

Version 2.0

Author: Progress 55 Ltd
Date: 14 September 2026
Classification: Internal / Schools

Version 2.0

Progress 55 Ltd — Assistant SENDCo

Based on Veritau Model Data Processing Addendum v2 (2022). Forked with Veritau's consent as a DPO customer of Progress 55 Ltd.

PARTIES

Progress 55 Ltd, a company incorporated in England and Wales under Companies House number **17045552**, with its registered office at **12 Mallard Way, Newcastle Upon Tyne, NE15 9DJ** ("the Provider")

and

The educational establishment (or multi-academy trust, local authority, or other contracting legal entity) entering into the primary Agreement with the Provider ("the Customer")

DEFINITIONS

Term	Meaning
Addendum	This Data Processing Addendum.
Agreement	The overarching contract for provision of services between the Provider and the Customer — the Pilot Agreement or the Master Services Agreement, as applicable — including its schedules.
Appropriate Safeguards	Has the meaning given in the UK GDPR.
Controller	Has the meaning given in the UK GDPR.
Data Loss Event	Any event that results or may result in unauthorised access to, loss of, or destruction of the Personal Data, including any Personal Data Breach.
Data Processing Schedule	Schedule 1 to this Addendum, which identifies the Personal Data and Data Subjects and sets out the scope, nature, purpose and duration of the Processing by the Provider.
Data Protection Impact Assessment	A risk assessment by the Controller of the impact of the envisaged processing on the protection and confidentiality of the Personal Data.
Data Protection Legislation	All applicable laws in the UK relating to data protection, processing of personal data and privacy, including the UK GDPR and Data Protection Act 2018 as amended from time to time.
Data Protection Officer	Has the meaning given in the UK GDPR.
Data Subject	Has the meaning given in the UK GDPR.
Personal Data	Has the meaning given in the UK GDPR.

Provider Personnel	All directors, officers, employees, agents and consultants of the Provider engaged in the provision of services under the Agreement.
Personal Data Breach	Has the meaning given in the UK GDPR.
Processor	Has the meaning given in the UK GDPR.
Processing	Has the meaning given in the UK GDPR. The terms Process, Processes and Processed will be construed accordingly.
Security Measures	Appropriate technical and organisational measures as detailed in Article 32 of the UK GDPR, to ensure the security of the Personal Data and prevention of a Data Loss Event, as documented in the Provider's Security Overview (current version available on request).
Subject Access Request	A request made by, or on behalf of, a Data Subject in accordance with rights granted under the Data Protection Legislation to access their Personal Data.
Sub-Processor	Any third party appointed to Process the Personal Data on behalf of the Provider in relation to the provision of services under the Agreement.
Transfer Risk Assessment	An assessment of the privacy and security risks associated with transferring the Personal Data to a territory that is outside the UK and EU.
UK GDPR	The retained version of the General Data Protection Regulation (EU 2016/679) as it forms part of UK law by virtue of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

1. INTRODUCTION

1.1 This Addendum and its Data Processing Schedule reflect the arrangements between the Parties for Processing of the Personal Data by the Provider on behalf of the Customer, in connection with the provision of services under the Agreement.

1.2 This Addendum forms an integral part of the Agreement and is incorporated into the Agreement by reference.

1.3 Both Parties shall comply with all applicable requirements of the Data Protection Legislation. This Addendum does not relieve, remove, or replace either Party's obligations under the Data Protection Legislation.

1.4 Each Party shall bear its own costs in relation to compliance with this Addendum and the Data Protection Legislation.

1.5 The Parties acknowledge that for the purposes of the Data Protection Legislation and this Addendum, the Customer is the Controller and the Provider is the Processor.

2. PROCESSOR OBLIGATIONS

2.1 Lawful Processing

2.1.1 The Processor will process Personal Data only in accordance with the Controller's written instructions unless the Processor is required to do otherwise by Law. If it is so required, the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law.

2.1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

2.2 Information Security

2.2.1 The Processor shall ensure appropriate technical and organisational measures are implemented to ensure the security of Personal Data held on behalf of the Controller, as documented in the Provider's Security Overview.

2.2.2 The Processor shall ensure that the Provider Personnel are subject to a contractual duty of confidentiality and do not process Personal Data except in accordance with this Addendum.

2.2.3 In respect of any Data Loss Event the Processor shall:

2.2.3.1 notify the Controller without undue delay, and in any event within seventy-two (72) hours of becoming aware of the event;

2.2.3.2 provide timely updates and information about the investigation of the Data Loss Event;

2.2.3.3 take reasonable steps to contain and mitigate the effects of the Data Loss Event; and

2.2.3.4 provide any reasonable assistance requested by the Controller.

2.3 Reasonable Assistance to the Controller

2.3.1 The Processor shall provide all reasonable assistance to the Controller in connection with:

2.3.1.1 compliance with Article 32 of the UK GDPR; and

2.3.1.2 the preparation of any Data Protection Impact Assessment that may be required prior to the commencement of the Processing under this Addendum.

2.3.2 In the event that the Processor receives a Subject Access Request or any other request from a Data Subject relating to their rights, the Processor shall:

2.3.2.1 notify the Controller without undue delay; and

2.3.2.2 provide any reasonable assistance requested by the Controller to comply with the Data Protection Legislation.

2.3.3 In the event that the Processor receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation, or any communication from the Information Commissioner's Office or any other regulatory authority in connection with Personal Data processed under this Addendum, the Processor shall:

2.3.3.1 notify the Controller without undue delay; and

2.3.3.2 provide any reasonable assistance requested by the Controller to comply with the Data Protection Legislation.

2.4 Sub-Processors

2.4.1 The Controller authorises the use of the Sub-Processors listed in Schedule 1.

2.4.2 The Processor shall enter into a written agreement with each Sub-Processor which shall contain terms equivalent to those set out in this Addendum such that they apply to the Sub-Processor.

2.4.3 The Processor shall remain fully liable for all acts or omissions of any Sub-Processor.

2.4.4 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-Processors, providing the Controller a minimum of fourteen (14) calendar days to object to such appointment on reasonable grounds relating to data protection.

2.4.5 In the event that the Controller objects to the appointment of a new Sub-Processor under clause 2.4.4 above, the Parties shall approach such concerns in good faith with a view to achieving resolution.

2.4.6 If the Parties are not able to achieve resolution under clause 2.4.5 above then the Controller may terminate the Agreement, including this Addendum, without penalty, and the Processor shall return or delete the Personal Data in accordance with clause 2.7.

2.5 International Transfers

2.5.1 The Processor shall only transfer Personal Data outside of the UK and EU if it has implemented Appropriate Safeguards to ensure the protection of the Personal Data in the destination territory, in accordance with the Data Protection Legislation.

2.5.2 In the event of any transfer of Personal Data outside of the UK and EU, the Processor shall carry out a Transfer Risk Assessment to determine that the Data Subject has sufficiently enforceable rights and effective legal remedies.

2.6 Audits

2.6.1 The Processor shall maintain and make available to the Controller upon request complete and accurate records and information to demonstrate its compliance with this Addendum and the Data Protection Legislation.

2.6.2 The Processor shall allow for audits and inspections by the Controller or the Controller's designated auditor, to establish the Processor's compliance with the terms of this Addendum. The Controller shall give reasonable notice (minimum fourteen (14) days) of any audit request. Audits shall be conducted during normal business hours and shall not unreasonably interfere with the Processor's operations.

2.7 Termination of the Agreement

2.7.1 Upon termination of the Agreement and at the written direction of the Controller, the Processor shall either delete or return the Personal Data to the Controller unless the Processor is required by Law to retain the Personal Data.

2.7.2 The Parties agree that the plan for return and destruction of the Personal Data once the Processing is complete is detailed in Schedule 1.

SCHEDULE 1 — DATA PROCESSING SCHEDULE

Description	Details
-------------	---------

Subject matter of the processing	Storage, retrieval, display, editing, quality review, and Word-document export of SEN Support Plans written by Customer staff for pupils with special educational needs or disabilities. Optional AI-assisted drafting and review of plan text, where the Customer has elected to enable it.
Duration of the processing	From the Effective Date of the Agreement until termination of the service relationship, plus any additional period required by Law. Deletion or return timeline set out below.
Nature and purposes of the processing	Nature: collection, recording, structured storage (encrypted ciphertext), retrieval, display, adaptation, alteration, use, transmission (to optional sub-processors for AI assistance), output as Word documents, and erasure. Purposes: (a) enabling Customer staff to record and maintain SEN Support Plans in line with the SEND Code of Practice 2015; (b) generating Word-document exports for Customer record-keeping, sharing with parents/carers, and statutory review processes; (c) providing deterministic and AI-assisted quality feedback on plan text; (d) Customer authentication and audit logging.
Type of Personal Data	Pupil data entered by Customer staff, which may include: pupil name, date of birth, year group, areas of need under the SEND Code of Practice 2015, diagnoses and outside-professional involvement (special category data under Article 9 UK GDPR), assessment observations, SMART outcomes and provisions, review and progress notes, access arrangements, pupil and family voice statements, and professional report recommendations. Customer staff data: full name, email address, display name, job role, multi-factor authentication tokens, audit log entries. <i>Note: the Service does not capture pupil, parent, or staff signatures. The exported Word document contains blank signature lines for the Customer to complete on the printed copy; any resulting handwritten signatures are held by the Customer on that physical document and are outside the scope of this Schedule.</i>
Categories of Data Subject	Pupils with special educational needs or disabilities enrolled at the Customer's educational setting; the parents, carers, and named family members of those pupils; Customer staff who author, review, or support plans (teachers, teaching assistants, SENCOs, SENDCos); outside professionals named within plan content (e.g. educational psychologists, speech and language therapists).
Plan for return and destruction of the data once the processing is complete UNLESS required to retain under UK law	The Service is end-to-end encrypted; plan content, plan titles and pupil identifiers reside in the Processor's infrastructure only as ciphertext, decryptable only by the Controller's users holding the relevant encryption keys. The Processor therefore cannot generate exports of Personal Data from outside the Service. Return and destruction proceeds as follows: (a) If the Controller wishes to retain Personal Data in a readable form, the Controller shall

	export all such Personal Data from the Service using the built-in Word-document export function before the Processor deletes the ciphertext. The export function is available to each authoring teacher for their own plans via the Review & Export step; the Controller's SENDCo coordinates multi-teacher exports by identifying the relevant plans on the SENDCo dashboard and requesting the authoring teachers to export, or by exercising the password-recovery flow where necessary. The Processor will provide reasonable technical assistance on request to enable the Controller to complete any such exports. (b) Within thirty (30) calendar days of the Controller's written direction, the Processor shall permanently delete all ciphertext copies of Personal Data from its infrastructure and certify the deletion in writing. (c) If no written direction is received within ninety (90) calendar days of termination of the Agreement, the Processor may delete the ciphertext after giving fourteen (14) calendar days' written notice to the Controller's Data Protection contact; this safeguard prevents Personal Data being retained indefinitely where a Controller ceases communication. (d) Audit log records may be retained for up to 730 days post-deletion in accordance with the Processor's data retention policy, to support security investigations and statutory obligations.
Authorised Sub-Processors	See Sub-Processor Register (maintained as a separate document and provided to the Controller on request). As at the Effective Date: Supabase Inc. (database hosting, UK — AWS London eu-west-2); Vercel Inc. (application hosting, EU routing); OpenAI LLC (optional AI-assisted drafting, United States — only when Customer staff explicitly opt in per browser session, with pupil names replaced with [PUPIL] and additional personal identifiers scrubbed before transmission); Resend Inc. (transactional email for staff account actions and security alerts, United States — staff email addresses only, no pupil data).

SIGNATURES

Controller (Customer)

Name of legal entity	
Authorised signatory name	
Role	
Signature	
Date	

Processor (Progress 55 Ltd)

Authorised signatory name	George Sayers
Role	Director
Signature	
Date	

This Addendum is a Schedule to, and forms part of, the agreement between Progress 55 Ltd and the Customer (the Pilot Agreement or, for paid use, the Master Services Agreement). Any conflict between this Addendum and the body of the Agreement is resolved in favour of this Addendum on matters of data protection.