TEACHGEN AI LTD

Standard Data Processing Addendum

Issued by TeachGen AI Ltd

Version	**2.0**
Effective date	**3 May 2026**
Document owner	**James Leeson, Data Protection Officer**
Sub-processor list	teachgen.ai/sub-processors
Contact	dataprotection@teachgen.ai

This is the standard form Data Processing Addendum issued by TeachGen AI Ltd. It is contractually referenced by the Service Agreement between TeachGen AI Ltd and the Customer. Sub-processor disclosures (Appendix B) are maintained at the URL above and updated under the change-notice procedure described in this document.

Background

This Data Processing Addendum ("DPA") forms part of the Service Agreement between **TeachGen AI Ltd** ("Supplier", "Processor") and the customer subscribing to the Services (the "Customer", "Controller") for the provision of AI-powered educational services ("Services").

(A) This Agreement is to ensure the protection and security of Personal Data that is the subject of this Agreement, including all Personal Data passed from the Customer (Data Controller) to the Supplier (Data Processor) for processing, or accessed by the Supplier on the Customer's authority for processing, or otherwise received by the Supplier for processing on the Customer's behalf.

(B) The Data Protection Laws place certain obligations upon a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the processing of the Personal Data carried out on its behalf is secure.

(C) This Agreement exists further to ensure that there are sufficient security guarantees in place and that the processing complies with obligations equivalent to those required by the Data Protection Laws.

(D) This Agreement further defines certain service levels to be applied to all uses of Personal Data and all Personal Data related services provided by the Supplier.

(E) The Services are typically deployed in educational settings and may process Personal Data of, or relating to, children. The Parties acknowledge the additional obligations arising under Article 8 of the Data Protection Laws and the United Kingdom's Information Commissioner's *Age Appropriate Design Code* (the "Children's Code").

(F) The Services incorporate AI processing. The Parties have agreed specific restrictions on the use of Personal Data for AI model training, set out in Clause 1.13.

(G) Definitions in this Background have the meanings given in the Agreement and/or the Data Protection Laws.

---

1. Data Protection

1.1 Definitions

In this Agreement:

- **Agreement** means this Data Processing Addendum, including all Appendices.
- **Authorised Users** means individuals with active platform access credentials issued by or on behalf of the Customer, including Customer staff and any Customer-authorised contractors.
- **Business Day** means any day other than a Saturday, Sunday or public holiday in England and Wales.
- **Children's Code** has the meaning given in Recital (E).
- **Customer Data** means all Personal Data collected, generated or otherwise processed by the Supplier as a result of, or in connection with, the provision of the Services. References to "Data" in this Agreement mean Customer Data.
- **Data Protection Laws** means:
  - the UK General Data Protection Regulation (UK GDPR) and any legislation which amends, re-enacts or replaces it in England and Wales;
  - the Data Protection Act 2018;
  - the Privacy and Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces it;
  - the EU General Data Protection Regulation (EU 2016/679) (EU GDPR) and any legislation which amends, re-enacts or replaces it; and

  - at all times, any other data protection laws and regulations applicable to a Party's processing of Personal Data under this Agreement.
- **Data Protection Officer** has the meaning given to it under Article 37 of the UK GDPR.
- **Data Subject** means an individual who is the subject of personal data.
- **EEA** means the European Economic Area.
- **Effective Date** means the date specified on the cover page of this Agreement, or the commencement date of the Service Agreement, whichever is later.
- **EU SCCs** means the standard contractual clauses for the transfer of personal data to third countries approved by Commission Implementing Decision (EU) 2021/914.
- **EU-US DPF** means the EU-US Data Privacy Framework, including its UK Extension, as administered by the United States Department of Commerce.
- **Losses** means direct costs, claims, demands, actions, awards, judgments, settlements, expenses, liabilities, damages and losses (including reasonable legal and other professional costs and expenses), but excluding indirect, consequential, special or punitive losses save where this Agreement expressly provides otherwise.
- **Personal Data** has the meaning given to it under the Data Protection Laws.
- **Records** has the meaning given in Clause 1.7.
- **Security Incident** has the meaning given in Clause 1.9.
- **Service Agreement** means the agreement between the Customer and Supplier and the quotation and service terms agreed to provide the Services.
- **Services** means the AI-powered educational platform and tools provided by the Supplier as described in the Service Agreement between the parties, and as further detailed in Appendix A.
- **Special Category Data** has the meaning given in Article 9 of the Data Protection Laws.
- **SubProcessor** has the meaning given in Clause 1.4.
- **Supervisory Authority** means any data protection authority with jurisdiction over the processing of the Data, including the United Kingdom's Information Commissioner's Office and any data protection authority of an EU member state.
- **Term** means the period during which the Service Agreement is in force.
- **Termination Date** means the date on which the Service Agreement ends or is terminated, howsoever caused.
- **Third Country** means a country, territory or international organisation outside the United Kingdom and the EEA.
- **UK Addendum** means the International Data Transfer Addendum to the EU Standard Contractual Clauses (B1.0) issued by the Information Commissioner's Office under section 119A of the Data Protection Act 2018.
- **UK IDTA** means the International Data Transfer Agreement (B1.0) issued by the Information Commissioner's Office under section 119A of the Data Protection Act 2018.

1.2 Data Processing

The Supplier shall comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done which might lead to a breach by the Customer of the Data Protection Laws.

The Supplier may only process Data to the extent it relates to:

- the types of Data;
- the categories of Data Subject;
- the nature and purpose,

set out in Appendix A of this Agreement and only for the duration specified therein.

Without prejudice to the above, the Supplier shall:

1. process the Data only in accordance with the written instructions of the Customer, unless the Supplier is required to process the Data for other reasons under the laws of the United Kingdom or European Union (or a member state of the European Union) to which Supplier is subject. If the Supplier is required to process the Data for these other reasons, the Supplier shall inform the Customer before carrying out the processing, unless prohibited by relevant law.
2. immediately inform the Customer if it believes that the Customer's instructions infringe the Data Protection Laws.
3. have in place, and maintain throughout the term at all times in accordance with the then current best industry practice, all appropriate technical and organisational security measures against:
   - unauthorised or unlawful processing, use, access to or theft of the Data; and
   - loss or destruction of or damage to the Data,

   to ensure that the Supplier's processing of the Data is in accordance with the requirements of the Data Protection Laws and protects the rights of the Data Subjects. On request the Supplier shall provide the Customer with a current written description of the security measures being taken (see Appendix C).
4. ensure that all persons authorised by the Supplier to process Data are bound by obligations equivalent to those set out in this Clause 1.
5. ensure that access to the Data is limited to:
   - those Supplier personnel who need access to the Data to meet the Supplier's obligations under the Agreement; and
   - in the case of any access by any Supplier personnel, such Data as is strictly necessary for performance of that Supplier personnel's duties.

The Supplier shall provide such assistance as the Customer requires in order for the Customer to:

- respond to requests relating to the Supplier's data processing from Data Subjects;
- ensure compliance with the Customer's obligations under the Data Protection Laws, including in relation to the security of processing;
- prepare any necessary data protection impact assessments and undertake any necessary data protection consultations.

1.3 International Transfers

The Supplier shall not transfer Data to a Third Country, nor permit a SubProcessor to do so, except where one or more of the following safeguards applies:

(a) **Adequacy.** The Third Country, sector or international organisation is the subject of a current adequacy decision under section 17A of the Data Protection Act 2018 (for UK-originating transfers) or Article 45 EU GDPR (for EEA-originating transfers), including the EU-US DPF where the recipient is currently certified under the relevant module.

(b) **UK transfers.** For UK-originating transfers, the Parties have entered into either the UK IDTA or the UK Addendum to the EU SCCs.

(c) **EEA transfers.** For EEA-originating transfers, the Parties have entered into the EU SCCs (Module 2: Controller-to-Processor where the Customer is the Controller and the Supplier the Processor; or Module 3: Processor-to-Processor as applicable).

(d) **Other Article 46 safeguards.** Another safeguard listed in Article 46 of the applicable Data Protection Laws is in place.

Where this Agreement is the executed transfer mechanism between the Parties:

- **UK transfers.** The UK Addendum is incorporated by reference. Tables 1, 2 and 3 of the UK Addendum are deemed completed using the Parties' details set out in this Agreement, the EU SCCs Module 2 (or Module 3 as applicable), the categories of data and processing in Appendix A, and the security measures in Appendix C. The Termination Date is the end date for Table 4.
- **EEA transfers.** The EU SCCs are incorporated by reference. Module 2 applies as between the Customer (data exporter, controller) and the Supplier (data importer, processor); Module 3 applies as between the Supplier and any SubProcessor. The optional docking clause is included. Clause 7 (docking clause) is included. Clause 9(a) Option 2 (general written authorisation) applies, with the change-notice period set at thirty (30) days. Clause 11(a) optional language is excluded. Clause 17 governing law is the law of the Republic of Ireland. Clause 18 forum and jurisdiction is the courts of Ireland. Annexes I, II and III are deemed completed using the Parties' details and Appendices A, B and C of this Agreement.

The Supplier shall, in respect of each SubProcessor located in a Third Country, identify in the Sub-Processor list at the URL in Appendix B the transfer safeguard relied upon. Where a SubProcessor's safeguard relies on a certification (such as the EU-US DPF), the Supplier shall update the published list within thirty (30) days if the certification status changes.

1.4 SubProcessors

The Supplier shall not engage any third party, except a member of the Supplier's group, to carry out processing in connection with the Services ("SubProcessor") without the Customer's prior written consent. The Customer's consent to the SubProcessors listed at the URL in Appendix B is granted by entering into this Agreement.

Prior to allowing a SubProcessor authorised under or in accordance with this Clause 1.4, including any member of the Supplier's group, to process any Data, Supplier shall enter into a written agreement with the SubProcessor under which the SubProcessor is obliged to comply with the terms of this Clause 1. The Supplier remains fully liable to the Customer for any acts or omissions of any SubProcessors.

The Supplier shall give the Customer not less than thirty (30) days' notice of any intended changes to the list of SubProcessors at the URL in Appendix B. The Customer may object in writing within that period; the parties shall then use good faith efforts to resolve the objection.

1.5 Information Provision and Audits

The Supplier shall make available to the Customer all information reasonably necessary to demonstrate compliance with this Agreement and the Data Protection Laws, in the following order of preference:

(a) **Independent audit reports.** On request and subject to a non-disclosure agreement, the Supplier shall provide the Customer with such independent assurance reports as the Supplier holds in respect of the Services from time to time, together with the equivalent reports held by its SubProcessors. The Supplier maintains a current list of its certifications and assurance reports at https://www.teachgen.ai/data-protection. The Supplier will notify Customers of material changes to its certification status. Where the Supplier has not obtained an independent certification in respect of a particular control, it relies on the certifications held by its enterprise SubProcessors. As of the Effective Date, this includes Microsoft Azure, Amazon Web Services and Google Cloud Platform, each of which holds current SOC 2 Type II and ISO 27001 attestations.

(b) **Security questionnaires.** The Supplier shall respond to reasonable Customer security and data protection questionnaires, including completing the Customer's standard supplier due diligence templates, within thirty (30) days of receipt.

(c) **SubProcessor evidence.** On request, the Supplier shall provide a summary of the assurance reports or certifications held by SubProcessors in respect of the Services, and shall exercise its audit rights against SubProcessors and share results with the Customer where reasonably required.

(d) **On-site audits.** Where (a) – (c) do not provide the Customer with sufficient assurance, the Customer (or a qualified third-party auditor selected by the Customer, reasonably acceptable to the Supplier and bound by appropriate confidentiality undertakings) may audit the Supplier's data processing facilities and practices relevant to the Services on no fewer than thirty (30) Business Days' written notice. Such audits shall:

- occur no more than once in any twelve (12) month period, except where required by a Supervisory Authority or where the Customer reasonably believes a Security Incident affecting the Customer's Data has occurred;
- be conducted during normal business hours;
- be limited to information, premises, systems and personnel relevant to the Services and the Customer's Data, and shall not extend to other customers' data, the Supplier's commercially confidential information, or SubProcessors' premises (in respect of which the Supplier shall instead exercise its rights under (c)); and
- be at the Customer's cost, save where the audit reveals a material breach of this Agreement, in which case the reasonable costs of the audit shall be borne by the Supplier.

(e) **Audit tail.** The Customer's audit rights under this Clause 1.5 survive termination of this Agreement for twenty-four (24) months from the Termination Date.

(f) **Supervisory Authority audits.** Nothing in this Clause 1.5 limits any right of audit or inspection vested in a Supervisory Authority by law, and the Supplier shall co-operate fully with any such audit.

1.6 Dealings with Supervisory Authorities

The Supplier shall promptly provide all assistance and information which is requested by any Supervisory Authority. The Supplier shall immediately notify the Customer of any request that it receives from any Supervisory Authority for assistance or information, unless prohibited by relevant law.

1.7 Records

The Supplier shall maintain records of all processing activities carried out on behalf of the Customer, including:

- the information described in Clause 1.5;
- where applicable, the name and contact details of the Data Protection Officer or representative based in the European Union of Supplier and of any SubProcessors;
- the different types of processing being carried out (if applicable);
- any transfers of Data outside of the EEA, including the identification of the relevant country or international organisation and any documentation required to demonstrate suitable safeguards;
- a description of the technical and organisational security measures referred to in Clause 1.2.3,

together, the Records ("Records").

The Records shall be in written electronic form. The Supplier shall provide the Records to the Customer promptly on request.

1.8 Data Subjects

On request, the Supplier shall take all necessary action and provide the Customer with all reasonable assistance necessary for the Customer to comply with the Customer's obligations under the Data Protection Laws in relation to:

- the provision of information to Data Subjects;

- the rectification of inaccurate Data in relation to a Data Subject;
- the erasure of a Data Subject's Data; and
- the retrieval and transfer of the Data of a Data Subject.

1.9 Data Breaches

The Supplier shall notify the Customer of any unauthorised or unlawful processing, use of, or access to the Data, or any theft of, loss of, damage to or destruction of the Data ("Security Incident"), or any breach of this Clause 1, **without undue delay, and in any event no later than seventy-two (72) hours of becoming aware, to ensure the Customer can meet its own Article 33 notification obligation**. Notification shall be sent to the Customer's registered data protection contact and copied to **dataprotection@teachgen.ai**. The notification shall include, to the extent then known, the categories and approximate number of Data Subjects and Data records affected, the likely consequences, and the measures taken or proposed to address the incident. Failure to notify the Customer in accordance with this Clause shall be deemed a material breach of this Agreement.

In the event of a Security Incident, the Supplier shall provide the Customer with full cooperation and assistance in dealing with the Security Incident, in particular in relation to:

- resolving any data privacy or security issues involving any Data; and
- making any appropriate notifications to individuals affected by the Security Incident or to a Supervisory Authority.

The Supplier shall investigate the Security Incident in the most expedient time possible and shall then provide the Customer as soon as possible thereafter with a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, and any other information that the Customer may request concerning the Security Incident.

The Supplier shall take all steps necessary to prevent a repeat of the Security Incident and shall consult with and agree those steps with the Customer unless immediate steps need to be taken and it is impractical to consult with the Customer in that respect.

1.10 Return or Deletion of Data

On the Termination Date, or earlier on the Customer's written request, the Supplier shall, at the Customer's choice:

(a) **Return** all Data to the Customer in a structured, commonly-used and machine-readable format (such as JSON or CSV), together with reasonable transition assistance, and confirm in writing that no copies remain (subject to (c) below); or

(b) **Delete** all Data, procure the deletion by SubProcessors of all Data, and confirm in writing that no copies remain (subject to (c) below).

The Supplier shall provide a thirty (30) day data export window from the Termination Date during which the Customer may exercise its rights under (a). Final return or deletion shall be completed within sixty (60) days of the Termination Date.

(c) **Permitted retention.** Where applicable law requires the Supplier to retain any Data, the Supplier shall: (i) notify the Customer of the legal requirement and the retention period; (ii) limit access to such Data to those persons strictly required to handle the legal obligation; and (iii) continue to protect the retained Data in accordance with this Agreement until deletion is permitted.

1.11 Warranties

The Supplier (Data Processor) warrants that:

- it will process the Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments, including the Data Protection Laws; and

- it will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Data and against the accidental loss or destruction of, or damage to Data to ensure the Customer's compliance with the Data Protection Laws.

The Supplier shall notify the Customer immediately if it becomes aware of:

- any unauthorised or unlawful processing, loss of, damage to or destruction of the Data;
- any advance in technology and best practice which mean that the Customer should revise the security and technical measures in place in order to protect the Data as well as the processing of the Data.

The Data Controller (the Customer) warrants that:

- it will provide the Supplier with all Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments, including Data Protection Laws;
- the Data which it supplies or discloses to the Supplier has been obtained fairly and lawfully; and
- it will obtain all necessary consents from persons whose Data is being processed and registrations with authorities to permit the Customer to transfer Personal Data to third parties pursuant to its obligations under this Agreement.

1.12 Liability and Indemnity

(a) **Mutual indemnity.** Each Party shall indemnify the other against Losses incurred by the indemnified Party as a direct result of a breach by the indemnifying Party of its obligations under this Agreement, to the extent such Losses are caused by that breach and could not reasonably have been mitigated by the indemnified Party.

(b) **Liability cap.** The aggregate liability of each Party under or in connection with this Agreement (including under this indemnity) is subject to the liability cap and exclusions set out in the Service Agreement. Nothing in this Agreement or the Service Agreement excludes or limits liability for: (i) fraud or fraudulent misrepresentation; (ii) death or personal injury caused by negligence; or (iii) any other liability that cannot lawfully be limited or excluded under English law.

(c) **Apportionment of administrative fines.** Where a Supervisory Authority imposes an administrative fine arising from circumstances for which both Parties bear responsibility, the Parties shall co-operate in good faith to apportion the fine in proportion to their respective fault, and each shall bear its own legal costs in dealing with the Supervisory Authority.

1.13 AI Training Restrictions

(a) The Supplier shall not use, and shall procure that its SubProcessors do not use, Customer Data to train, fine-tune, evaluate or otherwise improve any AI, machine-learning or generative model (whether the Supplier's, a SubProcessor's or any third party's), except where the Customer has given prior, specific and revocable written consent.

(b) For the avoidance of doubt, the restriction in (a) prohibits the use of Customer prompts, Customer Authorised User content, content created using the Services, or any derivative thereof, for any model-training purpose otherwise permitted by a SubProcessor's default terms.

(c) The Supplier shall configure its SubProcessor relationships (including any data-processing API agreements) so that data submitted via the Services is excluded from the SubProcessor's general training datasets. All AI inference performed under this Agreement (including text generation, image generation and any other generative AI features) is carried out within the Supplier's enterprise tenancy of its AI infrastructure providers — currently Microsoft Azure (including Azure OpenAI Service for text and image models), Amazon AWS, and Google Cloud Platform — in EU regions and under contractual training opt-out.

1.14 Special Category Data and Data of Children

(a) The Customer acknowledges that the Services are not designed for the routine processing of Special Category Data and that the Customer is responsible for ensuring an appropriate Article 9 lawful basis (including any required additional condition under Schedule 1 of the Data Protection Act 2018) before any Special Category Data is entered into the Services.

(b) The Customer acknowledges that the Services are typically used by educational institutions and that Personal Data of, or relating to, children may be processed. The Supplier shall apply the standards of the Children's Code to the design and operation of the Services, and shall provide such reasonable assistance as the Customer requires to comply with the Customer's obligations under the Children's Code and Article 8 of the Data Protection Laws.

(c) The Supplier shall apply enhanced operational safeguards (including restricted access, encryption at rest, and audit logging) to any Special Category Data and any data relating to children processed under this Agreement.

1.15 EU AI Act

The Supplier shall:

(a) classify the Services under the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) and notify the Customer of the classification on request;

(b) operate the Services in accordance with the obligations applicable to it as a provider or deployer (as the case may be) under the EU AI Act; and

(c) provide reasonable assistance to the Customer to enable the Customer to comply with the Customer's own obligations under the EU AI Act, including the provision of information necessary for the Customer to conduct fundamental rights impact assessments where applicable.

1.16 Priority

This Agreement applies in addition to the Service Agreement and any other contract between the Parties (whether currently in force or entered into in the future). In the event of any inconsistency between this Agreement and the Service Agreement (or any other contract between the Parties) in relation to data protection, this Agreement shall prevail.

Execution

This Addendum applies automatically as part of the Customer's Service Agreement with TeachGen AI Ltd from the effective date shown on the cover page. No counter-signature is required for the Addendum to take effect.

Customers requiring a counter-signed copy on the Customer's letterhead, or with the Customer's legal name and signatory pre-populated, may request one by emailing **dataprotection@teachgen.ai**. A counter-signed PDF will be returned within 5 business days.

TEACHGEN AI · STANDARD DPA

Appendix A — Schedule of Data Processing

Parties and Contacts

- **Supplier**: TeachGen AI Ltd (England and Wales)
- **Data Protection Officer**: James Leeson (dataprotection@teachgen.ai)
- **ICO Registration**: ZB619200
- **Customer contact for data protection notices**: As recorded by the Customer in its account settings, or such other address as the Customer notifies in writing.

Type of Data to be Processed under this Agreement

The Customer determines what personal data, if any, is entered into the platform. The Supplier does not require personal data for service functionality except for authentication purposes, and the Customer retains full control over what information is inputted by its Authorised Users.

The Supplier does not solicit Special Category Data and does not design the Services for the routine processing of such data; see Clause 1.14.

Categories of Data Subjects and Processed Data

Authorised Users with platform access

- Full name
- Work email address
- Job title / role
- Department / subject area
- School / institution name
- SSO identity identifiers and authentication metadata; no TeachGen password storage for school or trust users
- Platform usage data and activity logs
- Content created using the Services
- User preferences and settings

Indirect Data Subjects (data about, not from)

- Students
- Parents / guardians
- Other third parties

(Indirect references contained within content created by Authorised Users.)

Categories of Data Subject whose Data will be Processed

- Authorised Users with platform access
- Indirect references to students, parents / guardians, and other educational stakeholders (as contained within content created by Authorised Users)

Nature and Purpose of Processing

Primary purpose: Provision of the TeachGen AI educational platform Services as specified in the Agreement.

Specific purposes include:

- Enabling secure access to AI-powered educational tools

- Generating educational AI content such as (but not limited to) lesson plans, assessments, feedback, planning and reports based on user inputs
- Maintaining platform security and preventing unauthorised access
- Providing technical support and responding to service requests
- Improving service quality through aggregated usage analysis
- Ensuring compliance with applicable legal and regulatory requirements
- Fulfilling contractual obligations under the Service Agreement

Duration of Processing and Retention

The Supplier will process personal data from when the Customer starts using the Services until the Termination Date, plus the export and deletion windows set out in Clause 1.10. Per category retention is as follows:

Data category	Active retention	Post-termination
Authentication and account records	Term of the Agreement	Deleted within 60 days of Termination Date
Authorised User content (lesson plans, generated documents, prompts and outputs)	Term of the Agreement	Available for export for 30 days; deleted within 60 days of Termination Date
Platform usage and audit logs	12 months from event	Deleted within 60 days of Termination Date
Backup copies	Maximum 35 days rolling	Overwritten in normal backup cycle following Termination Date
Billing and tax records	Term of the Agreement	Retained for 6 years (UK statutory requirement) under restricted access

TEACHGEN AI · STANDARD DPA

Appendix B — Schedule of SubProcessors

The current list of SubProcessors engaged by the Supplier is published and maintained at:

https://teachgen.ai/sub-processors

The list at that URL forms part of this Agreement. The Customer consents to the engagement of the SubProcessors listed at that URL on the Effective Date of this Agreement, subject to the change-notice mechanism set out in Clause 1.4.

The Supplier shall give the Customer not less than thirty (30) days' notice of any intended addition or replacement of a SubProcessor by updating the list at the URL above and notifying registered Customer contacts. The Customer may object to such change within that period; the parties shall then use good faith efforts to resolve the objection.

A point-in-time snapshot of the SubProcessor list as at the Effective Date of this Agreement is available on request from the Data Protection Officer (dataprotection@teachgen.ai), and may be attached to a counter-signed copy of this Agreement at the Customer's request.

TEACHGEN AI · STANDARD DPA

Appendix C — Technical and Organisational Measures

Purpose of this document: These Technical and Organisational Measures ("TOMs") describe how the Supplier protects personal data in a transparent and lawful way. The Supplier's measures are based on industry best practices and legal requirements, taking into account the educational nature of the AI platform.

1. Data Privacy and Protection Measures

1.1 Governance and Leadership

- Ultimate accountability for data protection rests with the Supplier's leadership.
- Data Protection Officer: James Leeson (dataprotection@teachgen.ai)
- ICO Registration: ZB619200
- Clear roles and responsibilities are defined for managing personal data.

1.2 Policies and Procedures

The Supplier has implemented the following data protection policies:

- Data Protection Policy
- Privacy Notice (available at: https://www.teachgen.ai/privacy-policy)
- Data Protection Impact Assessment (DPIA) policy: the Supplier conducts a DPIA whenever materially new personal-data processing is introduced. The Supplier also maintains the public DPIA Support Pack to assist Customer DPIAs.

1.3 Data Processing Principles

- No profiling or automated decision-making occurs.
- No user evaluation or tracking for assessment purposes.
- Customer data is not used to train, fine-tune or evaluate any AI model. All AI inference is performed within the Supplier's enterprise tenancies on Microsoft Azure (including Azure OpenAI Service for text and image generation), Amazon AWS, and Google Cloud Platform, in EU regions, under contractual training opt-out (see Clause 1.13 of the Agreement).
- Teachers retain full professional control over AI-generated content.

1.4 Data Subject Rights

The Supplier maintains processes to handle data subject requests, including:

- Access requests
- Rectification of inaccurate data
- Data erasure
- Data portability

Records are maintained of all requests and responses.

1.5 Data Retention

- Personal data is processed during the service term plus thirty (30) days after termination.
- All data is deleted within sixty (60) days of termination unless legally required to be retained.
- No unnecessary data collection — only what is needed for authentication and service delivery.

2. Technical Security Measures

2.1 Data Encryption

- Data encrypted in transit using TLS 1.2 or above.
- Data encrypted at rest using AES-256 encryption.

2.2 Authentication and Access Control

- Single Sign-On (SSO) only — no password storage on the Supplier's side.
- Authentication is managed through the Customer's existing identity providers (Microsoft Azure Entra ID, Google Workspace).
- First-time login verification via email confirmation.
- Platform designed for educational professionals.

2.3 Infrastructure Security

- Cloud hosting with enterprise-grade security (Microsoft Azure EU-West region).
- Regular security monitoring and updates.
- 99.8% uptime target with scheduled maintenance notifications.
- Restricted access to systems on a need-to-know basis.

2.4 AI Model Security

- AI inference is performed within enterprise tenancies of the Supplier's AI providers (Microsoft Azure, AWS, GCP), which apply the providers' own content-safety filtering.
- The Supplier reviews AI-output safety as part of its release cycle.

3. Incident Response

3.1 Breach Detection and Response

- Logs are reviewed reactively in response to detected anomalies, using the cloud providers' built-in security tooling (such as Microsoft Defender for Cloud).
- Customer notification via dataprotection@teachgen.ai without undue delay and no later than 72 hours of becoming aware of a Security Incident, in accordance with Clause 1.9, so that Customers can meet the 72-hour Article 33 notification deadline that applies to them as Data Controllers.
- Root cause analysis and corrective action procedures.
- Co-operation with affected Customers in any onward notification to Supervisory Authorities and Data Subjects under Articles 33 and 34 of the Data Protection Laws.

3.2 Business Continuity

- Data backup and disaster recovery procedures.
- Emergency maintenance protocols with minimal notice when required.
- Service status communications via email and platform notifications.

4. Staff Training and Awareness

4.1 Employee Obligations

- All staff receive data-protection guidance on joining and have access to refresher materials maintained by the Data Protection Officer.
- Confidentiality agreements for all employees and contractors.
- Regular communication of policy updates and security best practices.
- Mobile device security policies for remote work.

5. Third Party Management

5.1 Sub-processor Oversight

- Written data protection contracts (Data Processing Agreements or equivalent) in place with all sub-processors.
- Regular assessment of sub-processor security measures.
- Thirty (30) day notice period for sub-processor changes (see Clause 1.4).

5.2 Current Sub-processors

See Appendix B (Schedule of SubProcessors) above.

6. Monitoring and Improvement

6.1 Regular Reviews

- Technical and organisational measures are reviewed at least annually, and following any material change to the Service or the Supplier's processing arrangements.
- Regular security assessments and updates.
- Monitoring of data protection compliance.
- Customer feedback integration into security improvements.

For questions regarding these measures, contact the Data Protection Officer at dataprotection@teachgen.ai.

TEACHGEN AI · STANDARD DPA

Appendix D — AI Risk Assessment and Mitigation Measures

Purpose of this document: Identifying potential data protection risks associated with the Supplier's AI platform and demonstrating the specific measures the Supplier has implemented to mitigate each risk. It supports customer due diligence and demonstrates the Supplier's compliance with GDPR risk assessment requirements.

Risk Factor	How This Applies to Our AI Application	User Impact	How We Protect Your Data
Evaluating or Profiling Users	Our AI application does not assess or rate users based on their input or activity.	Users are not being tracked or scored. Interactions remain private and are not used for profiling.	Only basic usage data (e.g. logins, feature usage) is collected. No profiling or user evaluation occurs.
Automated Decision-Making	Our AI application does not perform any automated decision-making activity.	Users maintain full control. The AI does not make choices on behalf of individuals.	The application provides tools for users to interact with; it does not replace human judgment or enforce decisions.
Tracking or Monitoring Users	We track individual usage, including login times and feature usage, to improve the app and ensure security.	Users' activity within the platform is logged for analytics, security, and service improvements. However, personal content entered into the system is not monitored.	Data is collected only for legitimate purposes such as security, service improvements, and analytics. Users are informed about tracking through our privacy policy. Access to usage logs is restricted to authorised personnel only.
Sensitive Information	Teachers might enter details about students (e.g. learning needs or lesson plans).	Risk of exposing confidential student or teacher data.	We use data encryption and allow schools to control what information is shared. Users should avoid inputting personal student data wherever possible to minimise this risk. We process data in the appropriate data centre regions to ensure compliance with Data Protection law. No training is performed on the data entered.
Merging Different Types of Data	We use secure sign-in (SSO) and may analyse feature usage patterns.	Users' data is not cross-matched with external sources in ways they wouldn't expect.	Data sources are kept separate, and only necessary data is used to improve the user experience.
[illegible]	[illegible] Word, PDF or Power- [illegible]	[illegible] access to key informa- [illegible]	[illegible]

Document control

- **Version**: 2.0
- **Effective date**: 3 May 2026
- **Document owner**: James Leeson, Data Protection Officer, TeachGen AI Ltd
- **Review cycle**: Annual, or sooner if required by changes in law or sub-processor arrangements
- **Sub-processor list**: https://teachgen.ai/sub-processors (versioned separately)
- **Contact for questions**: dataprotection@teachgen.ai