Ambertrace Labs Ltd

Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is entered into between:

- Ambertrace Labs **Ltd**, a company incorporated in England and Wales with company number [insert number] and registered office at [insert address] ("Ambertrace", "we", "us", "our"), acting as a Data Processor; and

- **The organisation engaging Ambertrace to provide Services** ("Controller", "you", "your"), acting as a Data Controller.

This DPA forms part of, and supplements, the Service Agreement, Terms and Conditions, Order Form, or other written or electronic contract between the parties (the "Agreement").

These Processing Terms apply where, in the course of providing Services under the Agreement, Ambertrace processes Personal Data on behalf of the Controller in accordance with Article 28 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

In the event of any conflict between this DPA and the Agreement, this DPA shall prevail to the extent the conflict relates to the processing of Personal Data.

---

1. Roles of the Parties

1.1 **Controller.** The Controller is the organisation that engages Ambertrace to provide Services. The Controller determines the purposes (the "why") and the essential means (the "how") of processing Personal Data. This includes deciding:

- which categories of individuals' data are collected (e.g. staff, students, service users, beneficiaries);

- what types of Personal Data are processed (e.g. names, contact details, safeguarding notes, usage logs); and

- the lawful basis under UK GDPR for processing such data.

1.2 **Processor (Ambertrace).** Ambertrace acts as a Data Processor when processing Personal Data on behalf of the Controller. Ambertrace shall:
(a) process Personal Data only on documented instructions from the Controller, unless required to do so by UK law or other applicable law;
(b) promptly notify the Controller if any instruction appears to infringe data protection law;
(c) not determine its own purposes for processing or use Personal Data for its own independent business purposes, except as strictly necessary to provide and improve the Services; and
(d) maintain records of processing activities carried out on behalf of the Controller, as required by UK GDPR.

1.3 Controller Responsibilities.

The Controller shall:

(a) ensure it has a valid lawful basis under the UK GDPR for all Personal Data it instructs Ambertrace to process;

(b) provide all necessary transparency information and privacy notices to Data Subjects, including any required consents;

(c) ensure that Personal Data supplied to Ambertrace is accurate, complete, and kept up to date;

(d) not input into the Services any categories of data which it is not lawfully permitted to process; and

(e) remain responsible for determining retention periods for Personal Data, subject to Ambertrace's obligations under this DPA.

---

2. Subject Matter & Duration

2.1 **Subject Matter.**
The subject matter of this DPA is the processing of Personal Data by Ambertrace in the course of providing the Services to the Controller. Such processing is limited to what is strictly necessary to deliver, configure, support, and improve the Services provided under the Agreement. This includes, without limitation:

- enabling access to and use of Ambertrace's platforms (including EddyAI MIND, EddyAI FLOW, Pilot2Work, Pilot4Justice, and related products or modules);

- processing user account information, login credentials, and usage activity to provide secure access;

- handling learner, student, employee, or service-user data for the purposes of safeguarding, employability, or service delivery, as instructed by the Controller;
- storing, hosting, transmitting, and backing up data within Ambertrace's systems;
- providing technical support, training, reporting, analytics, and system improvements; and
- complying with applicable legal, safeguarding, or regulatory requirements in connection with the Services.

2.2 **Duration.**
This DPA shall commence on the Effective Date of the Agreement and remain in effect for as long as Ambertrace processes Personal Data on behalf of the Controller under the Agreement. The DPA will automatically terminate when:
(a) all Services involving the processing of Personal Data have ended; and
(b) all Personal Data processed on behalf of the Controller has been securely returned or deleted in accordance with **Section 5(h) (Return or deletion of data)**.

For the avoidance of doubt, these Processing Terms shall continue to apply for as long as Ambertrace retains any Personal Data on behalf of the Controller, including during any data return or deletion period following termination of the Agreement, until such Personal Data has been securely returned or deleted in accordance with Section 5(h) (Return or deletion of data).

---

3. Nature & Purpose of Processing

3.1 Ambertrace shall process Personal Data solely for the following purposes, and only to the extent necessary to perform its obligations under the Agreement:

- (a) **Service delivery and configuration** – to enable authorised users to access and use the Services; to configure features, dashboards, and workflows; to host, store, and transmit data securely; and to provide user authentication, account administration, and platform functionality.
- (b) **Support and maintenance** – to provide technical assistance, troubleshooting, bug-fixes, training, and user guidance; to manage helpdesk requests; and to ensure continuity and reliability of the Services.
- (c) **System testing, security, and performance monitoring** – to monitor service stability, load, and response times; to conduct quality assurance, testing, and upgrades; to detect and prevent unauthorised access, misuse, fraud, or security threats; and to implement appropriate backup and disaster-recovery procedures.
- (d) Service improvements and analytics – to analyse aggregated or fully anonymised usage data (i.e. data that does not relate to an identified or identifiable individual) in order to enhance features, optimise workflows, and improve user experience. For the purposes of this clause, “anonymised” shall mean data that has been irreversibly de-identified in accordance with Recital

26 UK GDPR and the ICO's Anonymisation and Pseudonymisation Guidance, such that it is no longer Personal Data. Amberrace shall not rely on pseudonymised data for service improvement unless explicitly authorised by the Controller.

- (e) **Legal, safeguarding, and regulatory compliance** – to comply with applicable laws, regulations, statutory duties, and safeguarding obligations; to respond to lawful requests from regulators or authorities; and to retain records where required for child protection, employment law, financial record-keeping, or other mandatory purposes.

3.2 Amberrace shall not process Personal Data for its own marketing, profiling, or unrelated business purposes, and shall not further process Personal Data in a manner incompatible with the purposes set out above.

---

4. Categories of Data & Data Subjects

4.1 **Categories of Personal Data.**
Depending on the Services provided and the Controller's instructions, Amberrace may process the following categories of Personal Data on behalf of the Controller:

- (a) **Identification and contact data** – including first and last names, postal addresses, email addresses, telephone numbers, usernames, login credentials, authentication tokens, and user IDs.
- (b) **Demographic and organisational data** – such as age, date of birth, gender (if provided), job role, department, organisational affiliation (e.g. school, employer, local authority), learner status, and year group or programme enrolment.
- (c) **Account and usage data** – including activity logs, login history, time and duration of use, system interactions, user preferences, progress tracking, completion records, and audit trails.
- (d) **Educational, employability, or safeguarding data** – including records relating to educational attainment, individual learning plans, employability assessments, case management notes, safeguarding or welfare concerns, and any associated actions or interventions recorded by the Controller.
- (e) **Technical and device data** – such as IP addresses, device identifiers, browser type and version, operating system, diagnostic logs, crash reports, and information collected for the purposes of security, troubleshooting, and performance optimisation.
- (f) **Communications data** – including messages, comments, or feedback submitted through the Services, support requests, and correspondence between authorised users and Amberrace's support teams.
- (g) **Other data provided by the Controller** – any additional categories of Personal Data which the Controller elects to input into the Services in accordance with its own lawful basis for processing.

4.2 **Categories of Data Subjects.**
The Personal Data processed by Amberrace on behalf of the Controller may relate to the following categories of Data Subjects:

- (a) **Staff and professionals** – employees, teachers, trainers, mentors, social workers, administrators, or contractors engaged by the Controller.
- (b) **Students, learners, or young people** – individuals enrolled at an educational institution, referred by a local authority, or participating in employability, safeguarding, or rehabilitation programmes.
- (c) **Clients, beneficiaries, or service users** – individuals supported by the Controller in the context of social care, community programmes, employability schemes, or justice rehabilitation services.
- (d) **Parents, guardians, or emergency contacts** – where such information is provided by the Controller for safeguarding, pastoral, or communication purposes.
- (e) **Other authorised users** – any additional categories of individuals whose Personal Data is provided or made accessible by the Controller for use within the Services.

---

5. Obligations of Ambertrace (Processor)

Ambertrace shall comply with the obligations of a Data Processor under the UK GDPR, the Data Protection Act 2018, and other applicable data protection laws. In particular, Ambertrace shall:

(a) **Processing on instructions** – process Personal Data only on documented instructions from the Controller, including with respect to transfers of Personal Data to a third country or international organisation, unless required to do so by UK law or other applicable law. In such cases, Ambertrace shall inform the Controller of that legal requirement before processing, unless prohibited by law.

(b) **Confidentiality** – ensure that all persons authorised to process Personal Data (including employees, contractors, and Sub-Processors) are subject to an appropriate duty of confidentiality, whether contractual or statutory.

(c) **Security measures** – implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including (where appropriate): pseudonymisation and encryption of Personal Data; the ability to ensure ongoing confidentiality, integrity, availability, and resilience of systems; procedures for testing and evaluating effectiveness of security measures; and access controls to ensure Personal Data is only available to those with a business need to know.

(d) International transfers – Ambertrace shall not transfer Personal Data outside the United Kingdom (or, where applicable, outside the European Economic Area) without ensuring that appropriate safeguards are in place in accordance with applicable data protection law. Such safeguards may include:

(i) a decision of adequacy by the UK Government or the European Commission (as applicable);
(ii) the use of the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses (SCCs), as issued or approved by the Information Commissioner's Office; or
(iii) any other lawful transfer mechanism recognised under the UK GDPR or Data Protection Act 2018.

shall inform the Controller of the relevant safeguard relied upon prior to any such transfer and shall ensure that Data Subjects are afforded enforceable rights and effective legal remedies in accordance with Article 46 UK GDPR.

(e) **Assistance with Data Subject rights** – assist the Controller, insofar as possible, in fulfilling its obligation to respond to requests for the exercise of Data Subject rights under data protection law (including rights of access, rectification, erasure, restriction, portability, and objection).

(f) Personal Data Breaches – notify the Controller **without undue delay and in any event no later than seventy-two (72) hours** upon becoming aware of a Personal Data Breach, providing sufficient information to enable the Controller to comply with its obligations to notify regulators and/or Data Subjects. shall cooperate fully with the Controller in investigating, mitigating, and remediating the breach.

(g) **Demonstrating compliance** – make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the UK GDPR, and allow for and contribute to audits, inspections, or reviews conducted by the Controller or an appointed independent auditor. Any such audit shall:

(i) be subject to a minimum of thirty (30) days' prior written notice (except where earlier access is required by a regulator);
(ii) occur no more than once in any twelve (12) month period, unless a further audit is required due to a Personal Data Breach or material non-compliance;
(iii) be conducted during 's normal business hours and in a manner designed to minimise disruption to 's business operations; and
(iv) where an independent third-party auditor is appointed, such auditor shall be mutually agreed in advance by both parties and bound by appropriate confidentiality obligations.

(h) **Return or deletion of data** – at the end of the provision of Services, securely delete or return all Personal Data (at the Controller's choice), unless retention is required by law or permitted under this DPA. Where deletion is not technically feasible, shall ensure the data is securely protected from further processing.

---

6. Sub-Processors

6.1 **Use of Sub-Processors.**
may engage trusted third-party service providers ("Sub-Processors") to support hosting, infrastructure, security, analytics, and delivery of the Services.

6.2 **Flow-down obligations.**
shall ensure that all Sub-Processors are bound by written agreements imposing data protection

obligations that are no less protective than those set out in this DPA, including obligations regarding confidentiality, security, and breach notification.

6.3 **List of Sub-Processors.**
A current list of Sub-Processors is available on request. Ambertrace shall maintain this list and update it when changes occur.

6.4 **Notification of changes.**
Where Ambertrace intends to appoint a new Sub-Processor or replace an existing one, Ambertrace shall notify the Controller in advance (for example, by email or posting an update to the Sub-Processor list).

6.5 Right to object. If the Controller reasonably objects, on documented data protection or safeguarding grounds, to the use of a new Sub-Processor, the Controller may raise such objection within thirty (30) days of notification. Ambertrace will work in good faith with the Controller to address the objection. If no resolution can be reached, the Controller may terminate only the affected Services, provided such objection is not unreasonable or made in bad faith.

6.6 **Responsibility.**
Ambertrace remains fully responsible to the Controller for the acts, omissions, and compliance of its Sub-Processors with the terms of this DPA.

---

7. Data Breaches

7.1 Notification duty.
Ambertrace shall notify the Controller without undue delay, and in any event no later than seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller.

7.2 **Content of notification.**
Such notification shall include, where possible:
(a) a description of the nature of the Personal Data Breach, including, where feasible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records affected;
(b) the name and contact details of Ambertrace's Data Protection Officer (or other relevant contact point) from whom more information may be obtained;
(c) a description of the likely consequences of the Personal Data Breach; and

(d) a description of the measures taken, or proposed to be taken, by Ambertrace to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

7.3 **Cooperation.**
Ambertrace shall provide reasonable assistance to the Controller in investigating, containing, remediating, and mitigating the Personal Data Breach, and in complying with the Controller's obligations under applicable data protection law, including (where required) notifying the ICO and/or affected Data Subjects.

7.4 **Record-keeping.**
Ambertrace shall document all Personal Data Breaches, including the facts relating to the breach, its effects, and the remedial action taken, and shall make such records available to the Controller on request.

---

8. Special Provisions for Schools & Education Clients

Where the Controller is a school, trust, college, local authority, or other educational body, the following additional provisions shall apply:

(a) **Safeguarding obligations.** Ambertrace acknowledges that Personal Data may relate to children and young people, including vulnerable learners, and that such data is subject to heightened safeguarding and child protection obligations under UK law and statutory guidance (including *Keeping Children Safe in Education*).

(b) **Training and awareness.** Ambertrace will ensure that all staff and contractors who have access to child or learner data receive appropriate safeguarding and child protection training, proportionate to their role and level of access. Such training shall be refreshed at regular intervals.

(c) **Retention of learner data.** Unless otherwise required by law or expressly agreed with the Controller, retention periods for student or learner Personal Data will **normally not exceed seven (7) years unless statutory requirements or the Controller's documented retention policy requires otherwise**, after which time the data will be securely deleted or anonymised.

(d) **Support for safeguarding reporting.** Ambertrace will support the Controller in fulfilling its safeguarding reporting obligations by ensuring that the Services include functionality enabling admin users to monitor, flag, and review safeguarding concerns. Ambertrace shall not be responsible for making safeguarding decisions but will provide tools and training to enable Controllers to do so effectively.

(e) **Responsible use of AI outputs.** Ambertrace will ensure that any AI-generated outputs provided through the Services are clearly presented as supportive tools only. Such outputs must not be relied upon as a substitute for the professional judgment of teachers, Designated Safeguarding Leads (DSLs), social workers, or other qualified professionals.

(f) **Regulatory cooperation.** Amberlace shall cooperate with relevant educational and safeguarding authorities, where legally required, in relation to compliance investigations, safeguarding incidents, or data protection audits involving the Services.

---

9. Liability

9.1 The liability of each party under this DPA shall be subject to, and limited in accordance with, the exclusions and caps on liability set out in the main Service Agreement or Terms and Conditions between the parties.

9.2 For the avoidance of doubt:
(a) nothing in this DPA shall limit or exclude either party's liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, or any other liability which cannot lawfully be limited under applicable law;
(b) Amberlace shall remain fully liable to the Controller for the acts and omissions of its Sub-Processors to the same extent as if such acts or omissions were Amberlace's own; and
(c) the Controller remains responsible for ensuring that it has a lawful basis for providing Personal Data to Amberlace and for the accuracy, quality, and legality of that data.

---

10. Governing Law

10.1 This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it, its subject matter, or formation shall be governed by and construed in accordance with the laws of England and Wales.

10.2 The parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute, controversy, or claim arising out of or in connection with this DPA.

10.3 Nothing in this clause shall prejudice the statutory rights of Data Subjects or restrict the ability of either party to make a complaint to the UK Information Commissioner's Office (ICO) or any other competent data protection authority.