Ambertrace Labs Ltd

Privacy & Security Policy
Last updated: 28/05/2026

---

1. Introduction

Ambertrace Labs Ltd ("Ambertrace", "we", "us", "our") is committed to protecting the privacy, security, and integrity of personal data. We recognise that many of our clients operate in sensitive environments such as education, employability, justice, and safeguarding, and we take our responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 very seriously.

This Privacy & Security Policy sets out:

- how we collect, use, and protect personal data;
- the rights of individuals whose data we process;
- the technical and organisational measures we use to safeguard information; and
- how this Policy fits within our wider compliance framework.

This Policy should be read in conjunction with our other governance documents, which together form Ambertrace's compliance pack:

- **Terms & Conditions** – the core agreement governing use of our Services;
- **Data Processing Agreement (DPA)** – where we act as a Data Processor on behalf of a client organisation;
- **Acceptable Use Policy (AUP)** – setting out rules for safe and appropriate use of our Services by end users.

In the event of any inconsistency between these documents, the order of precedence is set out in our Terms & Conditions.

By using our Services, or by engaging with us as a client organisation, you acknowledge that you have read and understood this Policy.

2. Who We Are

Ambertrace Labs Ltd ("Ambertrace") is a UK-based artificial intelligence company that provides digital platforms and services to support education, employability, safeguarding, and justice programmes.

- **Company name:** Ambertrace Labs Ltd
- **Company number:** 15396088
- **Registered office address:** Ascend Co Working, 1st Floor Pentagon Shopping Centre, Chatham, ME4 4HY
- **Jurisdiction:** Incorporated in England & Wales
- **ICO Registration No :** CSN3223093 – Ambertrace is registered with the UK Information Commissioner's Office (ICO) as a data controller under the Data Protection Act 2018.
- **Data Protection Officer (DPO):** Matt Ledger
- **Privacy enquiries contact:** info@ambertracelabs.com

Ambertrace may act as either a Data Controller or Data Processor depending on the context in which we handle personal data. Further details of our role are set out in **Section 3 (Our Role in Data Protection)**.

Our commitment is to handle all personal data in compliance with the UK GDPR, the Data Protection Act 2018, and guidance issued by the ICO.

---

3. Our Role in Data Protection

Ambertrace operates in different capacities depending on the nature of the Services being provided and the context in which personal data is handled. Understanding this distinction is important for clients, end users, and data subjects.

- **Data Controller** – Ambertrace acts as a Data Controller when we determine the purposes ("why") and essential means ("how") of processing personal data. Typical examples include:
    - visitors to our websites;
    - individuals creating demo or trial accounts directly with Ambertrace;
    - direct subscribers to our Services where no separate client organisation is involved;

    - marketing, communications, and business development activities carried out by Ambertrace

- In these situations, we are responsible for ensuring that a lawful basis exists under UK GDPR, for providing privacy notices, and for fulfilling data subject rights requests directly.

- **Data Processor** – Ambertrace acts as a Data Processor when we process personal data strictly on the documented instructions of a client organisation such as a school, local authority, employer, or charity. Examples include:

    - learner, student, or service-user data entered into Ambertrace's platforms (e.g., EddyAI MIND, EddyAI FLOW, Pilot2Work, Pilot4Justice);

    - staff or mentor accounts created by a client organisation for its users;

    - safeguarding notes, assessments, or case data managed within our systems.

- In these cases, the client organisation is the Data Controller and remains responsible for establishing a lawful basis for processing, providing privacy notices to individuals, and determining retention periods. Ambertrace processes data as instructed by the Controller, in accordance with our **Data Processing Agreement (DPA)**.

Regardless of whether we act as Controller or Processor, we apply the same high standards of security and privacy protection across all personal data entrusted to us.

---

4. Categories of Data We Process

The types of personal data Ambertrace process depend on the nature of our relationship with you and whether we are acting as a Data Controller or Data Processor.

4.1 Identification and contact details

- Examples: name, email address, telephone number, postal address, job title, organisation.

- Context: collected when individuals create accounts, sign up for updates, participate in demos, or are registered by a client organisation.

4.2 Account and authentication data

- Examples: usernames, login credentials, authentication tokens, security questions, and access permissions.

- Context: required to provide secure access to Ambertrace's platforms and services.

4.3 Educational, employability, or safeguarding data (Processor role)

- Examples: student or learner profiles, attendance or attainment data, individual learning plans, employability assessments, case management notes, safeguarding concerns, and associated actions.

- Context: processed only when instructed by a client organisation such as a school, local authority, or employer. Ambertrace has no independent purpose for this data and acts solely on the Controller's instructions.

4.4 Technical and device data

- Examples: IP address, device identifiers, browser type and version, operating system, diagnostic logs, crash reports.

- Context: collected automatically to maintain system security, performance, and reliability.

4.5 Communications data

- Examples: enquiries, support requests, chat transcripts, messages submitted through the Services.

- Context: processed when users contact Ambertrace for assistance or interact within our platforms.

4.6 Feedback, analytics, and usage data

- Examples: product feedback, anonymised usage metrics, performance logs, aggregated statistical data.

- Context: used to improve functionality and user experience. Identifiable data is anonymised or aggregated before analysis, in line with ICO guidance.

4.7 Cookies and similar technologies

We use cookies and similar technologies on our websites to ensure they function properly, improve performance, and provide insights into how our Services are used. Some cookies are strictly necessary, while others (such as analytics or preference cookies) are optional and used only with your consent.

For full details of the cookies we use, the purposes they serve, and how you can manage your preferences, please see our [Cookies Policy] available on our website.

5. Purposes of Processing

We only process personal data where it is necessary, lawful, and proportionate to deliver our Services or meet our legal obligations. Depending on the context and whether we act as Controller or Processor, we may process personal data for the following purposes:

5.1 Service provision and configuration

- To enable authorised users to access and use Amberlace's platforms and features.
- To configure accounts, dashboards, workflows, and integrations in line with client requirements.
- To host, store, and transmit data securely.

5.2 User authentication and access management

- To verify the identity of users and provide secure logins.
- To administer role-based permissions and access controls.
- To prevent unauthorised access, misuse, or fraud.

5.3 Safeguarding, employability, and service delivery (Processor role)

- To support education, employability, safeguarding, and justice programmes as instructed by client organisations.
- To process learner, student, employee, or service-user data for case management, learning plans, or safeguarding reporting.
- Amberlace does not determine independent purposes for this processing.

5.4 Technical support and troubleshooting

- To respond to user support requests and resolve technical issues.
- To manage helpdesk tickets, bug reports, and feature queries.

- To train staff in providing effective support.

5.5 System stability, security, and performance monitoring

- To monitor service uptime, performance, and load.
- To conduct testing, upgrades, and quality assurance.
- To detect, investigate, and prevent security threats or misuse.
- To implement backup and disaster recovery procedures.

5.6 Analytics and service improvement

- To analyse anonymised and/or aggregated usage data to improve features, enhance functionality, and optimise user experience.
- Identifiable data is anonymised or aggregated before analysis in line with ICO guidance on anonymisation and pseudonymisation.
- Ambertrace will not use personal data for unrelated profiling, marketing, or resale.

5.7 Legal, regulatory, and safeguarding compliance

- To meet obligations under education, safeguarding, and employment law.
- To respond to lawful requests from regulators, authorities, or courts.
- To maintain statutory records (e.g., financial, safeguarding, or audit records).
-

---

6. Legal Basis for Processing (when acting as Controller)

When Ambertrace determines the purposes and means of processing personal data, we act as a Data Controller under the UK GDPR and the Data Protection Act 2018. In these circumstances, we rely on the following lawful bases:

6.1 Contractual necessity

- Where processing is required to deliver services that you subscribe to or request (e.g., account creation, platform access, support).

- Without this processing, we would be unable to fulfil our contractual obligations.

6.2 Legitimate interests

- Where processing is necessary to operate, maintain, and improve our services, provided such interests are not overridden by the rights and freedoms of data subjects.

- Examples include service analytics (in anonymised/aggregated form), fraud prevention, system monitoring, and ensuring network security.

- We apply a legitimate interest assessment (LIA) where appropriate to balance our interests against individual rights.

6.3 Legal obligations

- Where processing is necessary to comply with laws or regulations that apply to Ambertrace

- This may include safeguarding requirements, financial record-keeping, employment law, or responding to lawful requests from regulators or courts.

6.4 Consent

- In limited cases, we may rely on consent as the lawful basis for processing (e.g., sending marketing communications, collecting optional feedback, or participation in beta testing).

- Where consent is used, individuals have the right to withdraw consent at any time without detriment.

-

---

7. Sharing and Sub-Processors

7.1 Use of trusted providers

We may share personal data with carefully selected third-party service providers who help us deliver, secure, and maintain our Services. These may include hosting providers, cloud infrastructure platforms, support and helpdesk systems, analytics providers, and cybersecurity services.

7.2 Sub-processor obligations
Where we act as a Data Processor, any third-party providers we engage as Sub-Processors are bound by written agreements that impose obligations no less protective than those set out in our Data Processing Agreement (DPA). This includes requirements on:

- confidentiality,
- security standards,
- breach notification, and
- returning or deleting personal data at the end of the service.

7.3 Transparency of Sub-Processors
We maintain an up-to-date list of our Sub-Processors. This list is available to client organisations on request and is updated whenever a new Sub-Processor is appointed or an existing one is replaced. Clients will be notified in advance of material changes in accordance with our DPA.

7.4 No sale of personal data
Ambertrace does not sell, rent, or trade personal data to third parties under any circumstances. Any sharing of data is solely for the purposes set out in this Policy, our Terms & Conditions, and (where relevant) our Data Processing Agreement.

---

8. International Data Transfers

8.1 General approach
Ambertrace primarily seeks to process and store personal data within the United Kingdom or European Economic Area (EEA) wherever possible. However, some of our trusted service providers may operate outside these regions. In such cases, we ensure that appropriate safeguards are in place to protect personal data in line with the UK GDPR and the Data Protection Act 2018.

8.2 Safeguards used
Where personal data is transferred outside the UK/EEA, we rely on one or more of the following safeguards:

- **UK adequacy regulations** – where the UK Government has recognised that the destination country provides an adequate level of data protection.
- **International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses (SCCs)** – approved contractual safeguards that impose equivalent data

protection obligations on the recipient.

- **Other lawful transfer mechanisms** – such as explicit consent from the data subject (where appropriate), or transfers necessary for the performance of a contract or the establishment, exercise, or defence of legal claims.

8.3 Rights and remedies
Where we rely on safeguards, we ensure that data subjects have enforceable rights and effective legal remedies in relation to their personal data.

8.4 Transparency
Details of international transfers (and the safeguards used) are included in our Data Processing Agreement (when acting as Processor) and can also be made available to clients on request.

---

9. Data Retention

- **9.1 General principle**
  Ambertrace retains personal data only for as long as it is necessary to fulfil the purposes for which it was collected, or as required by law, regulation, or client instructions.
- **9.2 Adult users**
  For adult users (e.g., staff, professionals, or direct subscribers), personal data is retained only for the minimum period necessary to provide services and meet legal obligations (such as financial record-keeping).
- **9.3 Children and young people**
  Where we process the personal data of children or young people (for example, in education, employability, or safeguarding contexts), data may be retained for longer periods where required to meet safeguarding, child protection, or statutory duties.
- **9.4 Education settings**
  When acting as a Data Processor for schools, trusts, or local authorities, we follow the Controller's documented retention policies. Unless otherwise instructed or required by law, student or learner data will normally not be retained beyond **seven (7) years after the individual leaves the institution**, after which it will be securely deleted or anonymised.
- **9.5 End of processing**
  When personal data is no longer required, we ensure it is securely deleted or anonymised in accordance with recognised industry standards. Where deletion is not technically feasible, the data is placed beyond further use and protected from any unauthorised access or processing.

---

10. Data Subject Rights

10.1 Rights under UK GDPR

Individuals whose personal data we process ("Data Subjects") have the following rights under the UK GDPR:

- **Right of access** – to obtain a copy of their personal data and details of how it is processed.
- **Right to rectification** – to request correction of inaccurate or incomplete personal data.
- **Right to erasure ("right to be forgotten")** – to request deletion of personal data in certain circumstances (e.g., where it is no longer necessary for the purposes for which it was collected, or consent is withdrawn).
- **Right to restriction** – to request that processing is limited in certain circumstances (e.g., while a data accuracy challenge is resolved).
- **Right to data portability** – to receive personal data in a structured, commonly used, machine-readable format and, where feasible, to transmit that data to another controller.
- **Right to object** – to object to processing based on legitimate interests or to direct marketing.
- **Rights relating to automated decision-making** – to not be subject to decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects.

10.2 How rights are exercised

- **Where Ambertrace is a Data Controller** – Data Subjects may exercise their rights by contacting us directly at: [insert DPO email]. We will respond in line with UK GDPR timescales (normally within one month).
- **Where Ambertrace is a Data Processor** – requests must be directed to the relevant Data Controller (e.g., the school, local authority, employer, or other client organisation). Ambertrace will assist the Controller in fulfilling such requests, as required by our Data Processing Agreement.

10.3 Identification

To protect privacy, we may require individuals to verify their identity before responding to a rights request.

10.4 Limitations

Some rights may be subject to legal or contractual restrictions. For example, requests may be refused

where data must be retained by law, for safeguarding purposes, or for the establishment, exercise, or defence of legal claims.

---

11. Security Measures

11.1 Commitment to security

Ambentrade takes the security of personal data seriously. We implement technical and organisational measures designed to ensure a level of security appropriate to the risk, in line with the UK GDPR, the Data Protection Act 2018, and industry standards. Our approach is aligned with **Cyber Essentials certification** and informed by best practices such as **ISO/IEC 27001 principles**.

11.2 Key measures in place

Our security framework includes (but is not limited to):

- **Encryption** – personal data is encrypted in transit (TLS) and at rest (AES or equivalent) where applicable.
- **Access controls** – strict role-based permissions and the principle of least privilege are applied.
- **Authentication** – multi-factor authentication (MFA) is required for all administrator and privileged accounts.
- **Hosting security** – data is hosted with trusted providers that meet recognised security standards and are subject to regular independent audits.
- **Vulnerability management** – regular scanning, patching, and penetration testing to identify and remediate potential risks.
- **Logging and monitoring** – continuous monitoring of system access, activity, and anomalies, with alerts for suspicious or unauthorised activity.
- **Training and awareness** – staff receive regular training on safeguarding, data protection, and secure handling of personal data.
- **Business continuity and disaster recovery** – tested plans in place to maintain or restore services in the event of an outage, cyberattack, or other disruption.
- **Incident response** – a documented process to detect, report, and respond to security incidents, including compliance with breach notification obligations under UK GDPR.

11.3 Continuous improvement

We regularly review and update our security measures in light of technological developments, emerging threats, and evolving regulatory requirements.

---

12. Safeguarding in Education Settings

12.1 Commitment

Amberrace recognises that many of our clients operate in education, employability, and safeguarding contexts, where children, young people, and vulnerable learners are involved. We are committed to ensuring that our Services support, and never compromise, statutory safeguarding duties.

12.2 Staff training and awareness

- All Amberrace staff and contractors who may have access to learner or safeguarding data receive **safeguarding and child protection training**, proportionate to their role and level of access.
- Training is refreshed at regular intervals to ensure ongoing awareness of legal duties and good practice.

12.3 Safeguarding functionality in our platforms

- Our platforms include functionality that enables client administrators to **flag, review, and monitor safeguarding concerns** raised within the Services.
- Alerts and audit logs are provided to support Designated Safeguarding Leads (DSLs) and authorised staff in their decision-making.
- Amberrace does not make safeguarding decisions on behalf of clients but provides tools to support them in meeting their obligations.

12.4 Responsible use of AI

- Any AI-generated outputs provided through our Services are **clearly marked as support tools only**.
- Such outputs must not be relied upon as a substitute for the **professional judgment** of teachers, DSLs, social workers, or other qualified professionals.

12.5 Cooperation with authorities

Where legally required, Ambertrace will **cooperate with educational regulators, safeguarding authorities, or local child protection services** in connection with safeguarding incidents or investigations.

-

---

13. Data Breaches

13.1 Commitment

Ambertrace maintains procedures for detecting, investigating, and responding to actual or suspected personal data breaches. We treat all potential breaches with urgency and transparency.

13.2 Where Ambertrace is a Data Processor

- We will notify the relevant Data Controller **without undue delay and in any event within seventy-two (72) hours** of becoming aware of a Personal Data Breach.
- Our notification will include, where possible:
    - the nature of the breach and categories of data affected;
    - the likely consequences of the breach;
    - measures taken or proposed to address and mitigate the breach; and
    - a contact point for further information.
- We will cooperate fully with the Controller to investigate, contain, and remediate the breach, and to support the Controller in meeting its notification obligations to regulators and/or affected Data Subjects.

13.3 Where Ambertrace is a Data Controller

- We will assess the severity of any breach and notify the **Information Commissioner's Office (ICO)** without undue delay, and within 72 hours where required by law.

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also notify affected Data Subjects promptly and in clear, plain language.

13.4 Record-keeping
We maintain an internal breach log documenting the facts, effects, and remedial action taken for all breaches, whether or not notification is required.

---

14. Contact

14.1 Ambertrace contact details
For any questions, concerns, or requests regarding this Privacy & Security Policy, or the way Ambertrace handles personal data, please contact us:

- **Data Protection Officer (DPO):** Matt Ledger
- **Postal address:** Ascend Co Working, 1st Floor Pentagon Shopping Centre, Chatham, ME4 4HY
- **General enquiries:** info@ambertracelabs.com

14.2 Right to escalate
If you are not satisfied with how we handle your enquiry, you have the right to lodge a complaint with the **UK Information Commissioner's Office (ICO):**

- Website: https://ico.org.uk
- Telephone: 0303 123 1113
- Postal: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF