PRIVACY POLICY

AIENIKA – aienika.com

Version 1.0 • Dated 2026

This Privacy Policy explains how AIENIKA, a sole-trader academic mentoring practice based in England and trading under that name ("we", "us" or "our"), collects and uses personal data submitted through our website, aienika.com, and through subsequent email correspondence. We are the controller of that personal data and are registered with the Information Commissioner's Office. Our processing is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Our website is purely informational. It has no account area, no login, and no transactions. This policy covers visitors to the website and people who make an enquiry. Where an enquiry leads to an engagement, the processing of the mentee's personal data during the engagement is governed by the engaged-client terms in the Online Mentoring Agreement, to which we signpost below.

1. Personal data we collect

1.1 The enquiry form on the website collects four fields only: first name, last name, email address, and country. It collects no telephone number, no postal address, no information about a prospective mentee, and no other fields.

1.2 If you then correspond with us by email, we process the content of that correspondence and your email address. We do not use the website to collect special category (sensitive) data, and you should not send it to us through the form.

1.3 We do not use the website to collect personal data by analytics or tracking cookies. Wix Analytics is not enabled, Google Analytics is not in use, and no advertising or tracking tools are in use. See our Cookie Policy.

2. Why we use your data and our lawful basis

2.1 We use the data you submit to respond to and handle your enquiry and any resulting correspondence. Our primary lawful basis is our legitimate interests in dealing with enquiries about our services (Article 6(1)(f) UK GDPR); where you voluntarily contact us, consent operates as a secondary basis (Article 6(1)(a)). We carry out a balancing assessment when relying on legitimate interests and can provide details on request.

2.2 We do not use your data for marketing. We do not carry out individual profiling. We do not sell or share your personal data.

3. How long we keep your data

3.1 Enquiry-only data is retained for twelve months from your last contact, after which it is deleted. Where an enquiry becomes an engagement, the retention of engaged-client and safeguarding-relevant records is governed by the Online Mentoring Agreement and the Safeguarding Policy – in summary, session recordings are retained for six months, the signed Parental Consent Form for the duration of the engagement plus seven years, and other engaged-client records for up to six years.

4. Who we share your data with (sub-processors)

4.1 We use the following sub-processors. We allow them to handle personal data only where we are satisfied they protect it, and we impose contractual obligations to that effect:

Sub-processor	Role	Location / transfer basis	Notes
Wix	Website host and contact form	US / EU; UK GDPR safeguards (e.g. SCCs / UK Addendum) for any transfer outside the UK	–

CookieYes	Consent management platform; stores the consent log	Transfer safeguards under UK GDPR as applicable	See Cookie Policy
ProtonMail	Primary email correspondence	Switzerland; UK adequacy decision in place	–
Proton Drive	Working files arising from correspondence (session recordings are NOT held here)	Switzerland; UK adequacy decision in place	–
Microsoft 365 / Microsoft Teams	Video conferencing and storage of session recordings (where an enquiry leads to an engagement)	UK data residency; Microsoft Data Processing Agreement governs the relationship	Engagement only

4.2 We may also disclose personal data to professional advisers, or to law enforcement, courts, regulators or statutory authorities, where we are required to do so by law – including to local authority children's social care or the Local Authority Designated Officer in connection with a safeguarding concern. We do not otherwise share your data with any third party.

5. International transfers

5.1 Because our clientele is international, personal data may flow between a client's home jurisdiction and the UK. We process all personal data under UK GDPR. For transfers from the EU/EEA to the UK we rely on the European Commission's adequacy decision for the United Kingdom (June 2021); for Switzerland (Proton) we rely on the UK's adequacy decision. For jurisdictions without an adequacy decision (such as the United States, Singapore, or the UAE), we rely on appropriate safeguards under UK GDPR, such as the relevant Standard Contractual Clauses or the UK International Data Transfer Agreement / Addendum, supported by our own technical and organisational measures.

6. Our public commitments

6.1 We make the following commitments about how we treat your data: we send no marketing communications; we do not sell or share personal data; we do not carry out individual profiling; we do not train artificial intelligence on client data; and we do not use AI to draft correspondence – all mentor reports are written personally without AI assistance.

7. Children and the Children's Code

7.1 The website is intended for parents and prospective adult-age mentees, not for children. We nonetheless have regard to the ICO's Age Appropriate Design Code (the "Children's Code") in case a child visits: our data collection is minimal (the four form fields), we use no analytics or tracking, we apply data minimisation and privacy-by-default, we make no detrimental use of any child's data, and we do not profile. If we learn that we hold a child's data submitted without appropriate authority, we will delete it. During an engagement, the processing of a mentee's data is governed by the Online Mentoring Agreement and Safeguarding Policy and applies the Children's Code in detail.

8. Session recordings (engaged clients)

8.1 Where an enquiry leads to an engagement, all mentor sessions are recorded by video for safeguarding purposes. Recordings are retained within our Microsoft 365 tenant (UK data residency) and automatically deleted by a Microsoft 365 retention policy six months after the session. Access is restricted to the founder's account, protected by multi-factor authentication. Introductory consultations are not recorded. The lawful basis is our legitimate interests in safeguarding children (Article 6(1)(f) UK GDPR). The full recording policy is set out identically in the Safeguarding Policy, the Online Mentoring Agreement and the Parental Consent Form.

9. Your rights

9.1 Under UK GDPR you have the right of access; to rectification; to erasure; to restriction of processing; to data portability; to object to processing; and not to be subject to solely automated decisions with legal or similarly significant effects (we make no such decisions).

9.2 To exercise a right, email us by ProtonMail at aienika@pm.me. We aim to respond within seven working days and will in any event respond within the one-month statutory time limit. We may ask for enough information to confirm your identity.

9.3 Residents of the EU/EEA have equivalent rights under the EU GDPR. California residents have rights under the CCPA/CPRA, including to know, delete, correct, and opt out of “sale” or “sharing” of personal information (we do not sell or share). We honour equivalent rights for residents of other US states with comparable laws, including Virginia, Colorado, Connecticut, Utah, Texas and Florida.

10. Keeping your data secure

10.1 We use appropriate technical and organisational measures to protect personal data, including encrypted email and storage with Proton, UK-residency Microsoft 365 with multi-factor authentication, restriction of access to those with a genuine need, allowlisting of external Teams chat, and quarterly review of sign-in and admin logs.

10.2 We have procedures to deal with any suspected personal-data breach and will notify the ICO, and affected individuals, where we are legally required to do so – within 72 hours of becoming aware where feasible, in accordance with Article 33 UK GDPR.

11. How to complain

11.1 Please contact us first so we can try to resolve any concern. You also have the right to complain to a regulator: in the UK, the Information Commissioner’s Office (ico.org.uk, or 0303 123 1113); in the EU/EEA, your local supervisory authority; in California, the California Privacy Protection Agency; and in other US states, your state attorney general.

12. Changes to this policy

12.1 We may update this policy from time to time. When we make significant changes we will indicate them here and, where appropriate, notify you by email. This version supersedes any earlier version.

13. Governing law and jurisdiction

13.1 This policy is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction over any dispute arising in connection with it. This does not deprive a consumer resident in the UK or EU/EEA of the protection of any mandatory rule of their country of residence.

14. How to contact us

14.1 You can contact us by ProtonMail at aienika@pm.me with any question about this policy or the personal data we hold about you.