DIGITAL PALESTINE

Privacy Policy

Version: 2.0
Effective Date: 1 November 2026
Last Updated: 1 November 2026
Applies To: All members worldwide

What we collect, why, and the control you keep

> **Our promise, in one line**
> We practise data minimisation, we do not sell your personal data, and we do not run behavioural advertising surveillance. This Policy sits alongside the Terms of Service, the Cookie Policy, and the Community Communication & Ethics Charter.

1. SCOPE AND WHO CONTROLS YOUR DATA

1.1 This Policy explains how Digital Palestine ("we", "us") collects, uses, and protects personal information when you use the Service. The data controller is Handala CIC, a UK Community Interest Company (company number 17239783).

1.2 It applies to all members worldwide and forms part of your agreement with us together with the Terms of Service and the Charter.

2. INFORMATION WE COLLECT

The examples below illustrate the kinds of information involved - they are not a closed list. This Policy applies to all personal data we process about you, whether or not a specific example is named.

2.1 Information you give us

- **Account data:** name or public display name (pseudonym), email, password, age confirmation, and language. If you sign up, sign in or verify your account with a mobile phone number (for example through WhatsApp), we also collect that number and use it only to send you codes and keep your account secure.
- **Age Assurance data:** When you sign up, we check that you are 18 or over using facial age estimation. You take a short selfie in the app or browser, and a specialist age-check provider working for us uses it to estimate your age. The provider is certified under the UK Age Check Certification Scheme (ACCS). It does not identify you and does not compare your face with any database. A live check makes sure a real person is in front of the camera, not a photo or a video. The selfie is used only for the age check and is deleted as soon as the estimate is made. We keep only the result and the date. The provider may not use it for any other purpose. If the estimate cannot confirm that you are clearly over 18 (for example because you look under 25), you can prove your age another way, such as an identity document, which is checked and then deleted. You cannot use the platform until your age is confirmed.
- **Profile data:** optional details such as photo, bio, and interests; your ancestral village(s) or city/cities of origin in Palestine (up to two); your profession; and your current country of residence. Village of origin, ancestral ties, and related community affiliations can constitute "special category" data (ethnic or national origin, and potentially political opinion) under data-protection law - see Article 4.
- **Content:** posts, messages, images, audio, and video you create or upload.
- **Support and reports:** information you provide when you contact us or report content.

2.2 Information collected automatically

- **Usage and log data:** actions on the Service, pages viewed, and interactions, for operation, security, and safety.
- **Device and connection data:** device type, app version, identifiers, and IP address.
- **Approximate location:** derived from IP; precise location only with your explicit permission.
- **Cookies and similar technologies:** used for essential functions, security, and preferences (see Article 6).

2.3 Information from others

- Reports about your content from other members, and limited data from service providers used for security and abuse-prevention.

2.4 Family, ancestry and household data

- When you build or contribute to a family tree, create a “House,” or write a family story, we collect the information you add - including names, relationships, village/city ties, dates, photos, and narrative content. This can include information about relatives who are deceased or who have not registered for the Service themselves.
- If you add a living relative to a family tree, you confirm you have the right and any necessary consent to do so. A minor can only be added by a verified parent or legal guardian, as set out in Article 11. A person who discovers they (or a minor in their care) were added without consent can request correction, restriction, or removal through in-app tools or the contact in Article 10; we will act on verified requests.
- Village, city, and family-tree data can reveal an individual's location history or family network. Because of the safety risks this can carry for our community, family-tree visibility defaults to private/anonymised for minors and can be set to private by any member, and we apply the same government-request safeguards described in Article 24 of the Charter to this data.

2.5 Community, trust and governance data

- Your community memberships (village, country, and profession groups), Diwan membership and proposals, and the trust relationships in the Trust Key system (who has vouched for whom), which we use to run the community-moderation and content-filtering features described in the Charter.

2.6 Entity, verification and payment data

- If you register an Entity (business, organisation, or non-profit account), we collect the verification information you submit - such as the entity's mission, supporting documents, and contact details - to confirm its legitimacy before granting access.
- If you subscribe, or buy or sell in the Souks marketplace, your payment is handled by an independent third-party payment processor. We receive limited transaction metadata (amount, status, order reference) from the processor; we do not receive, store, or host your full card or bank account details on our servers.
- When we share data with technical infrastructure providers to support our systems, such sharing is strictly governed by robust Data Processing Agreements (DPAs) that restrict them from using your data for their own independent purposes.
- Identity-verification data under the "Hawiya" verification service will be governed by a dedicated policy, published before that feature launches, setting out exactly what is collected, how long it is kept, and the safeguards around it. Identity data submitted for "Hawiya" will not be linked to the user's public activity on the platform.

3. HOW WE USE INFORMATION

- To provide, maintain, and personalise the Service and your experience.
- To keep the community safe - detecting, reviewing, and acting on violations of the Charter, including threat detection.
- To secure accounts, prevent fraud and abuse, and protect rights and safety.
- To communicate with you about the Service, including safety notices, system updates, and optional direct communications, which operate strictly on an explicit opt-in basis.
- To comply with legal obligations and respond to lawful requests.
- We do not use your private content to build advertising profiles, and we do not sell your personal data.

4. LEGAL BASES FOR PROCESSING (WHERE THE GDPR APPLIES)

Some data central to the Service - such as ancestral village of origin, family relationships, and the “Occupied Palestine” location designation - can be “special category” data (revealing ethnic or national origin, and potentially political opinion) under Article 9 GDPR / UK GDPR. Where that applies, we rely on your explicit consent, given when you choose to provide that information, in addition to the bases below:

- **Performance of a contract** - to deliver the Service you signed up for.
- **Legitimate interests** - to keep the platform safe, secure, and functioning, balanced against your rights.
- **Legal obligation** - to meet our legal and regulatory duties.
- **Consent** - for optional features such as precise location; you can withdraw consent at any time.
- **Vital interests** - to protect someone from serious or imminent harm.
- **Explicit consent** - for special-category data such as ancestral origin and family relationships; you can withdraw this consent at any time by editing or deleting the relevant information in your settings.

5. HOW WE SHARE INFORMATION

- **With other members** - according to your privacy settings and the audiences you choose, including people you connect to through a village/city community, a Diwan, or a family tree or House.
- **With service providers (processors)** - who host, secure, translate and support the Service under contract and confidentiality (including our infrastructure providers), and may not use your data for their own purposes.
- **AI translation** - when you choose to translate a post, comment or message, its text is sent to Thaura, our AI translation provider, to produce the translation. Nothing is sent until you tap "Translate with Thaura". Thaura processes the text on servers in the European Union, does not use it to train its AI, and may not use it for any other purpose.
- **For legal and safety reasons** - to comply with law, respond to valid legal processes and requests for disclosure, enforce the Agreement, or protect members from harm.
- **In a business transfer** - if the Service is involved in a merger or acquisition, with notice to you.
- We do not sell personal data to third parties.

6. COOKIES AND SIMILAR TECHNOLOGIES

We use cookies and similar technologies (including on our mobile apps: local storage and device identifiers) for essential functions, security, and preferences. We do not use third-party advertising or cross-site tracking cookies. Full detail, including how to manage your choices, is in our separate Cookie Policy, which forms part of this Agreement.

7. DATA RETENTION

- We keep personal information only as long as needed to provide the Service, comply with legal obligations, resolve disputes, and enforce our agreements. We retain information suspected of constituting CSEA content or gathered from suspected child accounts to comply with legal obligations or to report suspected CSEA threats or offences.

Our default retention periods are:

- **Content and account data you delete** - purged or anonymised within 30 days of deletion, except where held briefly in secure backups (up to 90 days).
- **Closed accounts** - account data and content are deleted or anonymised within 30 days, other than data we must keep for legal, safety, or accounting reasons.
- **Evidence of imminent harm** - preserved for as long as legally required regardless of any deletion request.
- **Family-tree data about deceased individuals or non-users** - kept until an authorised family member or, for a living person, the individual themselves requests correction or removal, given its archival and genealogical purpose.
- **Moderation decisions and appeal records** - kept for 2 years to support consistency review and transparency reporting.
- **Payment and transaction records** - kept as required by our payment processor and by tax law (typically up to 6 years in the UK).

8. SECURITY

We implement strict technical and organisational measures - including encryption in transit and at rest, access controls, and continuous monitoring - to protect personal information. While no system is perfectly secure, we work diligently to protect your data and will notify you and relevant regulators of any significant data breaches within the timeframes required by law.

9. INTERNATIONAL TRANSFERS

Your information may be processed in countries other than your own, including outside the UK/EEA. Where that happens, we require recognised safeguards - such as the UK International Data Transfer Addendum or the EU Standard Contractual Clauses - to be in place with our infrastructure and hosting providers to protect it. Our AI translation provider, Thaura, processes text on servers in the European Union.

10. YOUR RIGHTS AND CHOICES

Depending on where you live, you may have the right to:

- Access the personal data we hold about you, and receive a copy.
- Correct inaccurate data, or complete incomplete data.
- Delete your data (“right to be forgotten”), subject to legal limits.
- Restrict or object to certain processing, including profiling.
- Port your data to another service in a structured format.
- Withdraw consent where processing is based on consent.
- Lodge a complaint with your local data-protection authority.

To exercise these rights, use in-app privacy controls or contact our Data Protection team at support@digitalpalestine.com. We respond within the timeframes required by law and do not discriminate against you for exercising them.

11. CHILDREN'S PRIVACY

The Service is strictly directed to adults and operates as an 18+ platform, in total alignment with Article 2 of the Terms of Service and the Community Charter. We do not intentionally create accounts, provide services to, or collect data from anyone under the age of 18. If we learn that an account has been created by a minor, it will be terminated immediately and all associated account data will be permanently deleted after 30 days save where retention is required for safety, legal or regulatory purposes and for reporting suspected child-safety violations.

The only instance where data relating to a minor may exist on the platform is when it is entered as genealogical information within a family tree or "House" by a verified parent or legal guardian who confirms their authority. In such cases, this data defaults to strictly private and anonymised to ensure maximum safety, as detailed in Article 2.4.

12. CHANGES TO THIS POLICY

We may update this Policy; we will post the new version and, for material changes, give additional notice. Continued use after changes take effect means you accept the updated Policy.

13. CONTACT

Privacy questions or requests: support@digitalpalestine.com

Digital Palestine
Privacy Policy
Version 2.0 | Effective 1 November 2026