DIGITAL PALESTINE

Community Communication & Ethics Charter

Version: 2.0
Effective Date: 1 November 2026
Last Updated: 1 November 2026
Applies To: Digital Palestine users and user-generated content
Minimum Age: 18 years
Governing Framework: Applicable law, including applicable law of England and Wales where relevant

---

1. PURPOSE AND STATUS OF THIS CHARTER

Digital Palestine is intended to provide an online space for Palestinian communities and individuals to communicate, share information, discuss public affairs, document experiences, exchange knowledge, and participate in lawful civic, cultural, academic, journalistic and human-rights dialogue.

This Community Communication & Ethics Charter ("Charter") establishes the standards that apply to communications and content on Digital Palestine.

The Charter forms part of the Digital Palestine governance framework and should be read together with:

- the Digital Palestine Terms of Service;
- the Privacy Policy;
- the Cookie Policy;
- the Moderation Policy;
- the Child Protection Policy;
- the "Before You Join" notice; and
- any additional policies or procedures published by Digital Palestine.

Where a provision of this Charter conflicts with mandatory applicable law, the mandatory legal requirement will prevail.

This Charter is intended to support lawful, responsible and respectful participation. It is not intended to suppress lawful political expression, journalism, academic research, historical discussion, human-rights documentation, peaceful advocacy or legitimate criticism.

2. ELIGIBILITY AND AGE REQUIREMENT

2.1 Adults Only

Digital Palestine is an 18+ platform.

Users must be at least 18 years old to create, maintain or use an account.

Digital Palestine does not intentionally provide accounts or services to persons under 18.

2.2 Age Assurance and Access Controls

Digital Palestine may use reasonable and proportionate measures to establish or assess whether a person meets the minimum age requirement.

The specific method used may depend on the risks associated with the service, applicable law, technical feasibility and data-protection requirements.

When a user signs up, Digital Palestine checks that the user is 18 or over using facial age estimation. The user takes a short selfie in the app or browser, and a specialist age-check provider working for Digital Palestine

uses it to estimate the user's age. The provider is certified under the UK Age Check Certification Scheme (ACCS). It does not identify the user and does not compare the user's 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. Digital Palestine keeps only the result and the date. The provider may not use the selfie for any other purpose. If the estimate cannot confirm that the user is clearly over 18 (for example, because the user looks under 25), the user can prove their age another way, such as with an identity document, which is checked and then deleted. A user cannot use the platform until their age is confirmed.

Digital Palestine will seek to minimise the amount of personal information collected for age-assurance purposes and will not use age-assurance information for unrelated purposes unless permitted by applicable law and properly disclosed.

Digital Palestine will periodically review whether its age restrictions and access controls remain effective.

2.3 Suspected Underage Accounts

If Digital Palestine has reasonable grounds to believe that an account is operated by a person under 18, it may restrict, suspend or terminate the account while the matter is reviewed.

Any personal information relating to an underage account will be handled in accordance with the Privacy Policy and applicable law.

The closure or deletion of an account does not necessarily mean that every associated record can be immediately erased, particularly where information must be retained for security, legal, fraud-prevention, dispute-resolution or other lawful purposes.

3. CORE COMMUNITY PRINCIPLES

Digital Palestine applies the following principles to community participation and content moderation.

3.1 Dignity

Users should communicate in a manner that respects the dignity and basic rights of other people.

3.2 Safety

Digital Palestine seeks to reduce reasonably foreseeable risks of serious harm, abuse, exploitation, threats and unlawful conduct.

3.3 Lawfulness

Users must comply with applicable law when using the platform.

3.4 Freedom of Lawful Expression

Digital Palestine recognises the importance of freedom of expression, including political, cultural, academic, journalistic and human-rights expression.

Lawful criticism of governments, states, public officials, political movements, institutions, ideologies, policies and armed actors is not prohibited merely because it is controversial, unpopular or politically sensitive.

3.5 Context and Proportionality

Content will be assessed in context wherever reasonably possible.

Digital Palestine will distinguish, where relevant, between:

- discussion and endorsement;
- reporting and promotion;
- documentation and glorification;

- criticism and incitement;
- historical reference and operational support;
- opinion and factual allegation;
- legitimate advocacy and unlawful conduct.

Enforcement measures should be proportionate to the seriousness and context of the relevant conduct, subject to applicable law and the need to protect users and the integrity of the service.

3.6 Authenticity and Accountability

Users should not use the platform to deceive others about their identity or affiliation.

Digital Palestine may permit the use of pseudonyms or public display names where permitted by the platform.

Pseudonymous participation does not permit impersonation, fraud, harassment or other prohibited conduct.

4. CONTENT AND CONDUCT THAT ARE NOT PERMITTED

Digital Palestine prohibits content or conduct that violates this Charter, the Terms of Service or applicable law.

The following categories are prohibited or may be subject to restriction.

4.1 Child Sexual Abuse Material and Child Exploitation

Digital Palestine prohibits:

- child sexual abuse material;
- sexual exploitation or sexualisation of children;
- grooming or solicitation of children;
- sexual services involving children;
- attempts to facilitate child exploitation; and
- other unlawful content involving child sexual exploitation.

Any such material may be removed immediately and, where required or appropriate under applicable law, reported to competent authorities.

4.2 Sexual Exploitation and Non-Consensual Intimate Content

Users may not publish or distribute:

- non-consensual intimate images;
- sexual content obtained through coercion or exploitation;
- sextortion material;
- threats to disclose intimate material;
- sexualised harassment; or
- content intended to facilitate sexual exploitation.

Because Digital Palestine is an 18+ platform, it may impose additional restrictions on explicit sexual content even where such content is not unlawful.

Non-explicit medical, educational, academic, journalistic, artistic or human-rights content may be treated differently where appropriate and lawful.

5. THREATS, VIOLENCE AND INCITEMENT

Digital Palestine prohibits:

- credible threats of violence;
- direct calls for unlawful violence against individuals or groups;
- instructions intended to facilitate violent criminal conduct;
- targeted threats intended to intimidate or coerce;
- coordination of unlawful violent activity; and
- content that unlawfully incites serious violence.

Discussion of violence, armed conflict, historical events, international humanitarian law, military operations, human-rights violations or political developments is not automatically prohibited.

Journalistic, academic, documentary and historical content may be permitted where it does not cross into unlawful incitement, facilitation or other prohibited conduct.

6. TERRORISM AND VIOLENT EXTREMISM

Digital Palestine recognises the legal framework against terrorism and prohibition on dissemination of terrorism-related content and will apply applicable law carefully and contextually.

6.1 Prohibited Conduct

Digital Palestine does not permit content or conduct that, where prohibited by applicable law:

- encourages, glorifies or incites terrorist violence;
- recruits individuals to participate in terrorist activity;
- provides operational instructions for terrorist violence;
- facilitates terrorist activity;
- provides prohibited material or practical support;
- celebrates or promotes terrorist violence in a manner prohibited by applicable law; or
- otherwise constitutes unlawful terrorism-related content.

6.2 Lawful Discussion and Documentation

The following may be permitted where lawful and appropriately contextualised:

- journalism;
- academic research;
- historical analysis;
- human-rights documentation;
- reporting on armed conflict;
- discussion of political organisations or armed actors;
- criticism of governments, organisations or political movements;
- discussion of terrorism legislation and policy;
- documentation of alleged violations; and
- discussion of victims and humanitarian consequences.

The mere mention, depiction, quotation or discussion of a person, organisation, symbol or event does not automatically constitute endorsement or unlawful support.

6.3 No Independent Political Designation

Digital Palestine does not independently determine that an individual or organisation is a terrorist organisation or terrorist actor.

Where applicable law imposes restrictions relating to a person or organisation, Digital Palestine will consider the relevant legal requirements and applicable official designations.

Moderation decisions will, where reasonably possible, consider the context, purpose, wording and apparent function of the content.

Sensitive cases may be escalated for human review.

Under the Terrorism Act 2000 it is an offence to express an opinion or belief that is supportive of a proscribed organisation while being reckless as to whether others will be encouraged to support it (section 12(1A)), or to publish an image of clothing or any other article in a way that arouses reasonable suspicion that the person is a member or supporter of a proscribed organisation (section 13(1A)).

7. POLITICAL EXPRESSION, JOURNALISM AND HUMAN-RIGHTS DOCUMENTATION

Digital Palestine is intended to permit lawful civic and political participation.

Subject to applicable law, users may engage in:

- political discussion;
- criticism of states and governments;
- criticism of political parties and movements;
- criticism of public officials;
- discussion of political ideologies;
- discussion of armed conflicts;
- peaceful advocacy;
- peaceful organising;
- petitions and civic participation;
- academic analysis;
- journalism;
- historical discussion;
- human-rights documentation;
- documentation of displacement and conflict;
- discussion of alleged violations of international law; and
- satire, parody and artistic expression.

Such content may be restricted where it independently constitutes prohibited conduct, including credible threats, unlawful incitement, recruitment, prohibited material support, targeted harassment or other unlawful activity.

Political disagreement, controversial opinions or criticism of a particular government or political position do not, by themselves, constitute violations of this Charter.

8. HATE SPEECH AND PROTECTED EXPRESSION

Digital Palestine prohibits targeted attacks or abusive conduct directed at individuals or groups on the basis of protected characteristics where the conduct reaches the applicable threshold for prohibited hateful or discriminatory content.

The platform distinguishes such conduct from legitimate discussion or criticism of:

- governments;
- states;
- political institutions;
- political movements;
- ideologies;
- religions as systems of belief;
- public policies; and
- political or military actors.

Users may express disagreement with ideas, policies or institutions, but may not use that distinction as a means of targeting individuals with prohibited abuse or threats.

Moderation decisions should consider context and avoid treating political disagreement as hate speech solely because it concerns a sensitive subject.

9. HARASSMENT, BULLYING AND COORDINATED TARGETING

Digital Palestine prohibits:

- targeted harassment;
- sustained abusive campaigns against an individual;
- credible intimidation;
- stalking or unwanted persistent targeting;
- threats or coercive campaigns;
- coordinated abuse designed to silence or intimidate a person;
- publication of private information for harassment; and
- abuse of platform reporting mechanisms to target another user.

The platform may take action against coordinated attempts to manipulate moderation systems, including mass-reporting campaigns intended to suppress lawful expression.

A report is an allegation, not proof of wrongdoing.

10. PRIVACY, DOXXING AND PERSONAL INFORMATION

Users must not publish another person's private or sensitive personal information without an appropriate lawful basis or legitimate justification.

This may include:

- private telephone numbers;
- private email addresses;
- residential addresses;
- precise real-time location information;
- identity documents;
- private photographs;
- private correspondence;
- financial information;
- account credentials;
- information facilitating stalking or physical targeting; and

- sensitive information obtained or disclosed for the purpose of harassment or harm.

Publicly available information is not automatically appropriate to republish.

Digital Palestine may restrict content where publication creates a significant privacy, safety or security risk.

11. FAMILY TREE AND THIRD-PARTY INFORMATION

Where Digital Palestine provides family-history or family-tree functionality, users must exercise particular care when entering information about other people.

Users must not use the feature to publish:

- sensitive information about non-users without appropriate justification;
- information about living children, unless you are their parent or guardian;
- private contact information;
- precise location information;
- identity documents;
- sensitive family information intended to facilitate harassment or harm; or
- information that is knowingly false and materially harmful.

Digital Palestine may limit, remove or redesign family-tree functionality where necessary to reduce privacy and safety risks.

12. GRAPHIC, DISTURBING AND CONFLICT-RELATED CONTENT

Digital Palestine may permit documentary, journalistic, academic or human-rights content depicting serious events where there is legitimate contextual or public-interest value.

However, users must not publish graphic material solely to shock, glorify violence, celebrate serious harm or encourage further violence.

Where appropriate, Digital Palestine may:

- restrict visibility;
- limit distribution; or
- remove content where it presents an unacceptable risk or violates applicable law.

13. MISINFORMATION, DECEPTIVE CONTENT AND MANIPULATED MEDIA

Digital Palestine does not intend to remove content merely because it is controversial, inaccurate, unpopular or disputed.

However, the platform may restrict content involving:

- deliberate deception;
- fraudulent impersonation;
- materially deceptive manipulated media;
- fabricated evidence presented as authentic;
- deceptive deepfakes likely to cause serious harm;
- coordinated deceptive campaigns; or
- false information used to facilitate unlawful conduct or serious harm.

Good-faith error, opinion, satire, academic debate, political disagreement and reasonable uncertainty should not automatically be treated as prohibited misinformation.

14. IMPERSONATION AND DECEPTIVE IDENTITY

Users may use pseudonyms or public display names where permitted.

Users may not impersonate another person, organisation or public authority in a manner intended to deceive, defraud, harass, manipulate or cause material harm.

Digital Palestine may require additional verification in cases involving suspected fraud, abuse, account takeover or serious impersonation.

15. FRAUD, SCAMS AND MANIPULATION

Digital Palestine prohibits:

- fraud;
- scams;
- phishing;
- deceptive financial schemes;
- fraudulent fundraising;
- credential theft;
- account takeover;
- deceptive commercial practices;
- manipulation intended to obtain money or valuable information unlawfully; and
- coordinated platform manipulation.

If Digital Palestine introduces fundraising or donation functionality, additional fundraising-integrity requirements may apply.

16. TRAFFICKING, SMUGGLING AND ILLEGAL ACTIVITIES

Digital Palestine does not permit content that facilitates unlawful trafficking, exploitation, smuggling or other serious criminal activity.

Educational, journalistic, academic and human-rights discussion of such conduct may be permitted where it does not facilitate the unlawful activity.

17. INTELLECTUAL PROPERTY

Users must not upload or distribute content in violation of applicable intellectual-property rights.

Digital Palestine may respond to valid copyright, trademark or other intellectual-property complaints in accordance with applicable law and its applicable complaint procedures.

Nothing in this Charter prevents lawful quotation, criticism, review, commentary, research, reporting or other legally protected uses of copyrighted material.

18. SPAM AND PLATFORM MANIPULATION

Users may not:

- send unsolicited bulk communications;
- operate deceptive automated accounts;
- artificially manipulate engagement;
- create accounts to evade enforcement;
- coordinate deceptive reporting;

- manipulate recommendation or ranking systems; or
- interfere with the technical operation of the platform.

19. USER RESPONSIBILITY

Users are responsible for the content they submit and the consequences of their unlawful conduct.

However, Digital Palestine does not treat user responsibility as a complete exclusion of the platform's own legal obligations.

Digital Palestine will operate its moderation, reporting, privacy and safety processes in accordance with applicable law and its published policies.

20. REPORTING AND BLOCKING

Users may report content or accounts that they believe violate this Charter or applicable law.

Reports should contain sufficient information to allow Digital Palestine to understand the concern.

Digital Palestine may:

- review the report;
- request additional information;
- restrict content temporarily;
- remove content;
- restrict an account;
- take no action where the report does not establish a violation; or
- escalate a matter where required or appropriate.

Users may also use available blocking or safety tools.

How to report, and what happens after a report, is explained in the Moderation Policy.

21. MODERATION AND ENFORCEMENT

Digital Palestine may use a combination of automated systems and human review.

Automated tools may assist with identifying potentially harmful or unlawful content but will not necessarily determine the final outcome in sensitive cases.

Depending on the circumstances, Digital Palestine may apply:

- reduced distribution;
- temporary restrictions;
- removal of content;
- account restrictions;
- suspension;
- termination; or
- referral to competent authorities where legally required or otherwise appropriate.

Enforcement should be proportionate to the seriousness of the conduct, taking into account relevant context.

22. SERIOUS AND IMMEDIATE RISKS

Digital Palestine may take immediate protective action where content or conduct presents a serious and immediate risk, including:

- credible threats of serious violence;
- child sexual exploitation;
- serious exploitation;
- account compromise;
- significant fraud;
- unlawful terrorism-related activity; or
- other circumstances requiring urgent intervention.

Where appropriate and legally permissible, the matter may subsequently be subject to human review or appeal.

23. APPEALS AND PROCEDURAL FAIRNESS

Where a moderation action is appealable, Digital Palestine will provide an appropriate mechanism for the affected user to request review.

How to appeal is explained in the Moderation Policy.

Appeals may be assessed based on:

- the relevant rule;
- the content and surrounding context;
- the user's explanation;
- new information;
- applicable law; and
- the proportionality of the original action.

Digital Palestine may maintain reasonable records of moderation and appeal decisions for accountability, security, quality assurance and legal compliance.

24. GOVERNMENT AND LAW-ENFORCEMENT REQUESTS

Digital Palestine may receive requests from governments, regulators, courts or law-enforcement authorities.

The platform will, where appropriate:

- assess whether the request is legally valid;
- identify the competent authority;
- consider the scope and necessity of the request;
- disclose only information that it is legally required or otherwise permitted to disclose;
- apply appropriate security measures; and
- notify the affected user where legally permissible and appropriate.

Nothing in this Charter requires Digital Palestine to comply with an informal request that has no valid legal basis.

Emergency procedures may apply where there is an immediate and serious risk to life or safety.

25. SECURITY AND ACCOUNT PROTECTION

Users should protect their account credentials and notify Digital Palestine promptly if they suspect unauthorised access.

Digital Palestine will seek to maintain appropriate technical and organisational security measures proportionate to the risks associated with the service.

No online service can guarantee absolute security.

26. TRANSPARENCY AND ACCOUNTABILITY

Digital Palestine may publish information about its moderation practices, significant policy changes, complaints and enforcement trends where appropriate.

Where transparency reporting is introduced, the platform will seek to provide meaningful information without compromising user privacy, security, confidential investigations or legal obligations.

27. LEGAL COMPLIANCE

This Charter is interpreted and applied in accordance with applicable law.

Digital Palestine does not represent that one policy can replace the laws of every country in which users may access the service.

Where mandatory legal requirements apply, Digital Palestine will take reasonable steps to comply with those requirements.

28. CHANGES TO THIS CHARTER

Digital Palestine may update this Charter from time to time.

Material changes will be communicated through appropriate means. The current version will identify its effective date and version number.

29. DOCUMENT HIERARCHY

This Charter should be read together with the Terms of Service, Privacy Policy, Cookie Policy and other applicable Digital Palestine policies.

Where there is an inconsistency:

- mandatory applicable law prevails;
- the Terms of Service govern contractual matters;
- the Privacy Policy governs personal-data processing;
- the Cookie Policy governs cookies and similar technologies; and
- this Charter governs community communication and content standards.

30. CONTACT

For questions concerning this Charter, moderation decisions, legal notices or community standards, users may contact:

Legal / Policy Contact: legal@handala.io
General Contact: support@digitalpalestine.com
Legal Entity: Handala CIC
Company / Registration Number: 17239783
Registered Office: C/O Melon Accountants Ltd, 96 Wilton Road, London SW1V 1DW, UK

Digital Palestine
Community Communication & Ethics Charter
Version 2.0 | Effective 1 November 2026