ACCEPTABLE USE POLICY (AUP)

DASHAMAP

Controlling Version (English)

Version: 1.1
Last Updated: June 21, 2026
Effective Date: June 21, 2026

Table of Contents

1. Purpose of the AUP, Scope, and General Principles
2. Operational Definitions
3. Permitted Use (Baseline)
4. Main Prohibitions (Prohibited Use)
5. Content and Data: Data Hygiene Rules
6. Special Rules for Business Customers, Professional Use, White Label, and Staff
7. Sparks, PDF Quota, Rate Limiting, Fair Use, and Resource Protection
8. Security: Minimum User Obligations
9. Sanctions, Export Control, Restricted Territories, and Geographic Compliance
10. Enforcement: Suspension, Termination, Review, and Remedies
11. Logging, Evidence, and Data Processing for Security/Enforcement
12. Reporting Abuse and Vulnerabilities (Responsible Disclosure)
13. Certified Astrologers, Partner/Dealer, Gift, Referral, Coupon, and One-Shot Safeguards
14. AUP Updates
15. Documentary Precedence, Interpretation, and Severability
16. Additional Protective Clauses
17. Governing Law and Venue
18. Controlling Language
19. Contacts

ACCEPTABLE USE POLICY (AUP) - DASHAMAP

This Acceptable Use Policy (the "AUP") sets forth the permitted and prohibited use rules for the DashaMap website, application, platform, workspaces, reports, exports, shared links, AI-assisted features, billing flows, professional tools, and related services (collectively, the "Service").

The AUP forms part of the DashaMap contractual framework and must be read together with the Terms of Service ("ToS"), Astrological Disclaimer, Privacy Policy, Cookie Policy, AI Transparency & Compliance Notice ("AI Notice"), Refund / Billing / Subscription / Credits Policy, and any applicable Data Processing Addendum ("DPA") or written agreement, where applicable.

The Service is operated by GLOBAL MOUNTAIN GROUP LLC, 30 N Gould St #39973, Sheridan, Wyoming 82801, U.S.A. Company ID: 2023-001208525. Official email: info@globalmountain.group. Website: www.globalmountain.group.

This AUP applies regardless of plan, access path, device, location, account type, product phase, or whether a feature is used for personal, professional, gift, one-shot, partner, dealer, certified astrologer, business, or white-label purposes. Features described in this AUP apply only where they are actually available, enabled, purchased, or expressly agreed in writing.

1. Purpose of the AUP, Scope, and General Principles

1.1 Objective of the AUP

The AUP exists to protect the Service, users, third parties, the Company, the technology supply chain, payment flows, and the integrity of DashaMap outputs. It is designed to prevent security abuse, economic abuse, misleading use, unlawful processing of personal data, unauthorized extraction, circumvention of Sparks/PDF quota rules, and misuse of symbolic or AI-assisted content.

1.2 Scope of application

This AUP applies to any use of the Service, including browsing protected areas, creating accounts, managing Souls/profiles, using My Path, Sinfonia, Oracle, Companion Soul, Child Evolution Atlas, gifts, one-shot digital reports, PDF exports, Magic Links, referral/coupon tools, Certified Astrologers features, Partner/Dealer tools, business features, white-label/client tools, and AI-assisted features, where available.

1.3 Acceptance and contractual incorporation

Users accept this AUP in the manner provided by the ToS, including by creating an account, purchasing or activating paid features, accepting clickwrap/checkbox terms, using protected features, or continuing to use the Service after an effective update, subject to mandatory law.

1.4 Enforcement guiding principles

The Company applies this AUP using criteria of proportionality, severity, urgency, recurrence, risk, impact on other users or systems, fraud indicators, available logs, and reasonable contractual or technical evidence.

1.5 Nature of the Service

DashaMap is a symbolic, educational, reflective, narrative, and edutainment-oriented digital service. Deterministic engines may calculate time-based structures, while AI may assist with narration, explanation, summarization, or reformulation. The Service must not be used as a sole or automated basis for medical, psychological, legal, financial, credit, insurance, employment, child welfare, veterinary, or other high-impact decisions.

2. Operational Definitions

- "Abuse" means any use that violates this AUP, the ToS, applicable policies, law, or reasonable security/economic integrity rules.
- "Sparks" means DashaMap usage units used for eligible paid or premium functions, including AI-assisted or interpretive functions where applicable.
- "Included Sparks" means Sparks included with an active plan for the relevant billing period.
- "Purchased Sparks" or "Add-on Sparks" means Sparks purchased separately through authorized payment flows.
- "Promotional Sparks" means bonus, referral, courtesy, gift, campaign, or other non-purchased Sparks.
- "PDF quota" means included or purchased entitlement for eligible PDF/report exports, where available.
- "Consumption Event" means a successful billable or Sparks/PDF-consuming event according to product logic.
- "Scraping / Crawling / Data Mining" means automated, systematic, or semi-systematic extraction of pages, outputs, reports, metadata, APIs, assets, content patterns, or Service behavior.

- "Reverse Engineering" means attempting to reconstruct code, prompts, pipelines, calculation logic, model routing, security controls, internal architecture, or proprietary methods.
- "Circumvention" means bypassing, evading, or manipulating plan limits, Sparks balances, PDF quota, paywalls, authentication, link expiration, security controls, anti-fraud checks, or technical protections.
- "AI Misuse" means using AI-assisted features or outputs for prohibited generation, model training, dataset creation, prompt extraction, safety bypass, deceptive claims, or unauthorized competitive benchmarking.
- "Shareable Link" or "Magic Link" means any Service-generated link or access mechanism for viewing, downloading, sharing, or redeeming content.
- "Professional Use" means use by astrologers, consultants, business users, Partner/Dealer participants, Certified Astrologers, or any user sharing outputs with clients or third parties.
- "Suspected Violation" means a situation where reasonable technical, contractual, payment, usage, or behavioral signals indicate possible violation before final assessment.
- "Confirmed Violation" means a violation supported by reasonable technical, contractual, documentary, payment, or behavioral evidence.

3. Permitted Use (Baseline)

3.1 General rule

The Service may be used only for lawful, authorized, contractually permitted, and Service-consistent purposes.

3.2 Examples of permitted use

- creating and managing lawful accounts, Souls/profiles, settings, preferences, and notes;
- using My Path, Sinfonia, Oracle, Companion Soul, Child Evolution Atlas, and similar functions within the active plan and available entitlements;
- generating or downloading reports, PDFs, exports, one-shot reports, and Magic Links through official flows;
- purchasing and using subscriptions, gifts, one-shot products, Add-on Sparks, and PDF quota through authorized checkout flows;
- sharing outputs with authorized recipients through official functions, while respecting privacy and confidentiality;
- using professional or business features only where enabled, purchased, approved, or agreed in writing.

3.3 General user responsibility

Users remain responsible for account activity, credentials, entered data, third-party data, downstream sharing, local legal compliance, professional claims, and the interpretation or use of outputs.

4. Main Prohibitions (Prohibited Use)

4.1 Violations of law and third-party rights

- fraud, scams, phishing, deception, impersonation, money laundering, unlawful collection of data, or unlawful processing of third-party data;
- infringement of intellectual property, copyright, trademarks, trade secrets, image rights, privacy, confidentiality, publicity rights, or contractual rights;
- defamation, harassment, stalking, intimidation, discrimination, threats, or unlawful manipulation;
- creation of false testimonials, false reviews, false endorsements, deceptive public claims, or content falsely attributed to real persons or entities.

4.2 Scraping, harvesting, and unauthorized automation

- scraping, crawling, harvesting, mining, indexing, or archiving any part of the Service, outputs, PDFs, reports, links, pages, endpoints, assets, or metadata;
- using bots, scripts, browser automation, extensions, unauthorized APIs, or coordinated accounts to extract content or produce outputs at scale;
- automating requests to farm Sparks value, generate bulk reports, create archives, or bypass normal user flows;
- using the Service as a source for unauthorized databases, corpora, benchmarks, prompt packs, or competing services.

4.3 Reverse engineering, probing, and attacks

- decompiling, disassembling, probing, fuzzing, brute-forcing, credential stuffing, scanning, or testing production systems without written authorization;
- attempting SQL injection, XSS, SSRF, CSRF, prompt injection, command injection, path traversal, privilege escalation, auth bypass, or equivalent attacks;
- accessing or attempting to access data, accounts, tenants, reports, links, or environments belonging to other users;
- interfering with logs, monitoring, telemetry, watermarking, anti-fraud, rate protection, or security controls;
- conducting denial-of-service, stress testing, artificial load, or any activity likely to degrade availability.

4.4 Bypassing Sparks, PDF quota, plans, paywalls, and economic controls

- manipulating Sparks or PDF quota counters, balances, request IDs, checkout events, generation state, delivery state, refunds, or accounting records;
- exploiting bugs, race conditions, double-clicks, retries, stale sessions, or timing issues to obtain paid outputs without valid consumption or payment;
- creating duplicate accounts, false identities, coordinated usage, self-referrals, or artificial transactions to bypass plan or promotion rules;
- reselling, trading, transferring, or monetizing Sparks, PDF quota, gifts, links, or benefits outside official authorized features;
- using abusive chargebacks or bad-faith disputes after receiving paid features, reports, Sparks, or outputs.

4.5 Anti-training and anti-dataset clause

- using DashaMap outputs, reports, timelines, texts, PDFs, structures, prompts, naming systems, or patterns to train, fine-tune, evaluate, benchmark, or improve AI/ML systems;
- creating datasets, corpora, prompt libraries, style replicas, report packs, or competing templates from Service outputs;
- systematically extracting outputs to infer prompts, model behavior, calculation logic, routing logic, or product style;
- performing unauthorized competitive benchmarking, model-evaluation farming, or service comparison designed to reproduce or replace DashaMap.

4.6 Unauthorized sharing, links, and access

- publishing Magic Links or reports publicly where they contain personal, confidential, private, gift-recipient, child, pet-owner, client, astrologer, partner, or business data;
- sharing credentials, sessions, accounts, admin panels, staff access, partner/dealer tools, or certified astrologer access in violation of the ToS or plan rules;
- removing watermarks, disclaimers, notices, attribution, expirations, or access controls;
- using false identities or unauthorized contact details to obtain, claim, or access gifts, reports, subscriptions, dashboards, applications, or partner/dealer benefits.

4.7 Brand misuse, white-label misuse, and prohibited claims

- presenting DashaMap as medical, psychological, psychiatric, therapeutic, veterinary, legal, financial, tax, investment, employment, insurance, credit, scientific, or government-certified advice;
- claiming guaranteed accuracy, guaranteed outcomes, certain prediction, diagnosis, treatment, professional certification, or official endorsement where not expressly granted;
- using white-label, partner, dealer, certified astrologer, referral, coupon, or public profile tools to conceal material limitations or make deceptive claims;
- using DashaMap trademarks, logos, screenshots, reports, badges, rankings, or references in a misleading or unauthorized manner.

4.8 High-impact use restrictions

The Service and outputs must not be used as the sole or automated basis for decisions affecting health, therapy, child welfare, veterinary care, legal rights, financial investments, tax, employment, insurance, credit, eligibility, discipline, housing, public benefits, safety, or similarly significant matters. Qualified human review and independent professional advice are required where appropriate.

5. Content and Data: Data Hygiene Rules

5.1 Strictly prohibited data

- passwords, API keys, access tokens, seed phrases, OTP codes, recovery codes, private keys, or credentials;
- full payment card data or bank data outside authorized payment-provider flows;
- malware, exploit code, harmful payloads, or instructions intended to attack, compromise, or sabotage systems;
- illegal material, exploitation material, abusive material involving minors, non-consensual intimate material, or content facilitating criminal conduct;
- third-party data that the user knows or reasonably should know they have no lawful basis or authorization to process.

5.2 Unnecessary and strongly discouraged data

Users must avoid entering unnecessary sensitive or excessive data in prompts, notes, applications, support tickets, gifts, partner/dealer notes, certified astrologer materials, client data, or free-text fields.

- health diagnoses, therapy records, medical reports, psychological or psychiatric details, veterinary medical details, or crisis information;
- religion, philosophical beliefs, political opinions, trade-union data, sexual orientation, biometric data, criminal data, or other special-category data unless strictly lawful and necessary;
- full identity document numbers, bank accounts, tax identifiers not requested by official billing flows, trade secrets, confidential third-party materials, or data of minors without lawful authority.

5.3 Dangerous or prohibited content

- hate, terrorism, violence, self-harm promotion, threats, harassment, stalking, exploitation, illegal sexual content, fraud, defamation, deceptive claims, or rights-infringing content;
- content that turns symbolic outputs into instructions for dangerous, unlawful, professional, or high-impact action;
- prompts or workflows designed to evade safeguards, obtain disallowed outputs, or generate misleading professional claims.

5.4 User warranty

By entering data or content, the user represents that they have the rights, consents, authority, lawful basis, mandate, or other legal title necessary to do so, including for third-party data, child data, pet-owner data, client data, gift-recipient data, professional application data, and partner/dealer data.

6. Special Rules for Business Customers, Professional Use, White Label, and Staff

6.1 Availability only where enabled

Business, white-label, staff, client portal, API, enterprise, and professional features apply only if and when enabled, purchased, approved, or agreed in writing. The existence of this AUP does not guarantee that any such feature is publicly available.

6.2 Access and role governance

- assign least-privilege access and revoke access when staff leave or roles change;
- adopt internal rules for sharing, Magic Links, exports, client data, retention, and downstream disclosures;
- protect admin, staff, partner/dealer, certified astrologer, and business dashboards from unauthorized access;
- ensure authorized users comply with this AUP, the ToS, Privacy Policy, DPA where applicable, and downstream obligations.

6.3 Third-party data and lawful basis

Professional and business users must have a valid lawful basis, mandate, engagement, consent, notice, or other authority before entering or processing third-party data. They remain responsible for privacy notices, consents, data subject rights, confidentiality, and lawful downstream use.

6.4 Downstream disclaimers and communications

Professional users must not present outputs as guaranteed, certified, scientific, medical, legal, financial, veterinary, therapeutic, or high-impact advice. They must provide appropriate disclaimers and human review where outputs are shared with clients, end customers, families, pet owners, or the public.

7. Sparks, PDF Quota, Rate Limiting, Fair Use, and Resource Protection

7.1 No artificial daily cap on available Sparks

DashaMap does not use artificial daily consumption caps solely to prevent a user from spending legitimately available Sparks or PDF quota. If the user has available Sparks, PDF quota, or purchased entitlements and the feature is authorized, those entitlements may be used according to product rules and available infrastructure.

7.2 Permitted technical protections

The Company may still apply technical, security, anti-fraud, idempotency, duplicate-click prevention, balance verification, authorization, abuse prevention, payment-risk, provider-protection, infrastructure-stability, and incident-containment controls. These controls are not commercial daily caps; they are protective measures intended to prevent abuse, fraud, duplication, unauthorized access, technical failure, or service degradation.

7.3 Fair use and anomalous usage

Abuse may include use patterns that are artificial, automated, coordinated, deceptive, technically harmful, or inconsistent with normal authorized use, even when the account still has Sparks or paid entitlements.

- mass automated generations, PDF exports, one-shot purchases, gift claims, or Oracle/Deep requests;
- batch-factory behavior designed to create archives, datasets, resale content, or competing libraries;
- coordinated use across multiple accounts to evade security, billing, promotion, or partner/dealer rules;
- use of scripts, bots, or repeated retries to trigger duplicate delivery, duplicate refunds, duplicate Sparks restoration, or chargeback leverage.

7.4 Failed delivery and consumption integrity

If a Sparks-consuming or PDF quota-consuming task fails due to a Service-side technical error before producing a usable output, the treatment of Sparks/PDF quota is governed by the Refund / Billing / Subscription / Credits Policy. Users must not exploit retries, failures, or restoration mechanisms to obtain duplicate outputs or free value.

8. Security: Minimum User Obligations

- use strong, unique passwords and enable MFA/2FA where available;
- protect devices, browsers, sessions, admin access, staff access, partner/dealer access, and certified astrologer credentials;
- not share credentials, sessions, OTP codes, links, or private dashboard access;
- promptly report unauthorized access, suspected compromise, suspicious billing activity, or exposed links;
- not bypass security warnings, access controls, payment verification, fraud checks, or technical safeguards.

9. Sanctions, Export Control, Restricted Territories, and Geographic Compliance

Users may not use the Service in violation of sanctions, export controls, embargoes, trade restrictions, or applicable compliance rules. The Company may apply proportionate technical screening, anti-fraud signals, approximate geolocation, payment-risk checks, and access restrictions where reasonably necessary and lawful. Use of VPNs, proxies, TOR, or masking tools to evade compliance restrictions may violate this AUP.

10. Enforcement: Suspension, Termination, Review, and Remedies

10.1 General enforcement framework

For suspected or confirmed violations, the Company may take measures based on severity, risk, urgency, recurrence, payment risk, technical indicators, and impact.

10.2 Possible measures

- warning or request for remediation;
- additional verification, access challenge, or ownership confirmation;
- temporary limitation of features, Sparks use, PDF exports, AI functions, gifts, one-shot reports, links, dashboards, partner/dealer tools, or certified astrologer tools;
- suspension or termination of account, tenant, public profile, partner/dealer status, referral/coupon benefits, or professional listing;
- revocation of links, exports, reports, watermarks, or public access;

- blocking of IPs, devices, sessions, payment attempts, or risk signals where lawful and proportionate;
- reporting to payment providers, authorities, or affected parties where required or reasonably necessary.

10.3 Immediate measures without notice

Immediate measures may be applied without prior notice for attacks, mass scraping, data exfiltration, fraud, payment abuse, chargeback abuse, unauthorized access, systematic circumvention, severe AI misuse, serious privacy risk, or imminent harm.

10.4 Review request

Except in cases of manifest fraud, legal restriction, or serious ongoing risk, a user may request reconsideration by writing to info@globalmountain.group with the affected account, date/time, contested measure, explanation, and relevant evidence. Reconsideration does not guarantee reinstatement and does not automatically suspend the measure.

10.5 Effects on Sparks, subscriptions, and refunds

During security or anti-fraud review, the Company may temporarily freeze features or balances. In confirmed fraud or violation cases, improperly obtained Sparks, PDF quota, credits, outputs, promotions, gifts, referral benefits, partner/dealer commissions, or certified astrologer benefits may be voided to the extent permitted by law. Valid remedies for Service-side technical failures remain governed by the Refund / Billing / Subscription / Credits Policy and mandatory law.

11. Logging, Evidence, and Data Processing for Security/Enforcement

To protect the Service, users, payments, entitlements, and legal rights, the Company may process technical and security data such as logs, timestamps, IP/device/session indicators, account events, checkout events, Sparks/PDF consumption records, delivery records, refund records, partner/dealer attribution records, referral/coupon events, support records, abuse signals, and enforcement records. Such processing is governed by the Privacy Policy, Cookie Policy, and applicable law.

12. Reporting Abuse and Vulnerabilities (Responsible Disclosure)

12.1 Abuse reporting

Reports may be sent to info@globalmountain.group with subject "AUP - Abuse report". Include, where available, affected account/tenant, date/time, URLs, screenshots, logs, description, and estimated impact.

12.2 Responsible disclosure

The Company accepts responsible, non-destructive vulnerability reports. This AUP does not authorize active testing of production systems, access to third-party data, destructive testing, exfiltration, denial-of-service, public exploit disclosure, or any activity that creates material risk without written authorization.

12.3 No bounty or unlimited safe harbor

Absent a separate written agreement, this AUP does not create a bug bounty, compensation right, or unlimited safe harbor. Any doubt must be resolved conservatively by reporting without exploitation.

13. Certified Astrologers, Partner/Dealer, Gift, Referral, Coupon, and One-Shot Safeguards

13.1 Certified Astrologers

Certified Astrologers features, if available, are subject to application, review, approval, payment, publication, suspension, and removal rules. Users and applicants must not submit false credentials, misleading claims, fake reviews, fake testimonials, false country/city information, unauthorized third-party photos, deceptive professional claims, or guaranteed-result promises. Public profile metrics, visits, rankings, popularity, badges, or directory placement are not guarantees of competence, revenue, contacts, or results.

13.2 Partner/Dealer and referral/coupon tools

Partner/Dealer and referral/coupon tools, if available, must not be used for fake accounts, self-attribution, self-referral abuse, duplicate-account schemes, traffic manipulation, misleading promotions, guaranteed-result promises, unauthorized use of customer personal data, or commission fraud. Partner/Dealer notes and internal records must not contain unnecessary personal data such as private emails, phone numbers, birth data, maps, questions, profiles, or sensitive client information unless an official field and lawful basis expressly require it.

13.3 Gifts

Gift features must not be used for spam, harassment, phishing, identity abuse, unwanted messaging, public posting of private gift links, or collection of recipient data without lawful basis. Gift buyers are responsible for entering accurate recipient information and avoiding unnecessary personal or sensitive data in gift messages.

13.4 One-shot reports

One-shot products are for authorized digital delivery through official flows. Users must not automate one-shot purchases, generate reports for unauthorized persons, resell bulk reports, abuse retries, exploit failed deliveries, or use chargebacks to retain delivered content without payment.

14. AUP Updates

The Company may update this AUP for technical, legal, security, anti-fraud, product, pricing, provider, compliance, or operational reasons. Updated versions will be published with the applicable version, Last Updated date, and Effective Date. Material changes may be notified through reasonable channels where required by law. Continued use after the effective date constitutes acceptance, subject to mandatory rights.

15. Documentary Precedence, Interpretation, and Severability

This AUP supplements the ToS. In case of apparent conflict, the Privacy Policy prevails for personal data processing, the Cookie Policy prevails for cookies/tracking tools, the Astrological Disclaimer and AI Notice prevail for symbolic/AI limitations and non-reliance, the Refund / Billing / Subscription / Credits Policy prevails for Sparks/PDF quota, refunds, billing, and delivery remedies, the ToS prevails for general contractual matters, and this AUP prevails for use restrictions, security, anti-abuse, and enforcement. Mandatory non-waivable rights remain unaffected.

Examples in this AUP are non-exhaustive. If any provision is invalid or unenforceable, the remaining provisions remain effective to the maximum extent permitted by law. Failure to enforce a rule immediately does not waive future enforcement.

16. Additional Protective Clauses

16.1 No agency / no partnership / no representation

Nothing in this AUP creates an agency, partnership, joint venture, employment, mandate, fiduciary, franchise, or representative relationship. Users, Partner/Dealer participants, Certified Astrologers, business users, and professional users may not bind the Company toward third parties unless expressly authorized in a written agreement signed by the Company.

16.2 No general monitoring duty

The Company may implement safeguards, moderation, logging, review, and anti-abuse controls, but does not assume a general obligation to monitor all user content, prompts, outputs, downstream use, professional claims, partner/dealer activity, certified astrologer communications, or shared links in real time, except as required by law.

16.3 Cost recovery for severe abuse

To the extent permitted by law, severe abuse such as attacks, mass scraping, fraud, data exfiltration, systematic circumvention, or payment manipulation may result in claims for documented and reasonably necessary containment, investigation, remediation, legal, security, and compliance costs, without limiting other remedies.

16.4 Survival

Rules that by nature should survive suspension or termination remain effective, including anti-abuse, anti-scraping, anti-training, IP, logging/evidence, enforcement, cost recovery, no waiver, controlling language, and protection of Company and third-party rights.

17. Governing Law and Venue

Governing law, venue, dispute resolution, and consumer-right rules are governed by the ToS. Mandatory consumer protections and non-waivable rights under applicable law remain unaffected.

18. Controlling Language

This English version is the controlling and legally binding version of this AUP, unless the Company expressly designates another controlling version in writing. Translations are provided for convenience only. In case of discrepancy, the controlling English version prevails, subject to mandatory local law.

19. Contacts

GLOBAL MOUNTAIN GROUP LLC
30 N Gould St #39973, Sheridan, Wyoming 82801, U.S.A.
Company ID: 2023-001208525
Email: info@globalmountain.group
Website: www.globalmountain.group

Recommended subject lines: "AUP - Abuse report", "Security Report - DashaMap", "Partner/Dealer Compliance - DashaMap", "Certified Astrologer Compliance - DashaMap".

END OF AUP DOCUMENT