

USA

- [DIGITAL MILLENNIUM COPYRIGHT ACT \(DMCA\) POLICY](#)
- [TERMS OF SERVICE — SECTION: FEES, SUBSCRIPTIONS AND BILLING, DISPUTE RESOLUTION AND ARBITRATION AGREEMENT](#)
- [US PRIVACY POLICY & STATE LAW DISCLOSURES](#)
- [CONSUMER HEALTH DATA PRIVACY POLICY](#)
- [ACCEPTABLE USAGE POLICY](#)

DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) POLICY

Effective Date: September 8, 2026

IQBID Helios Limited ("Company," "we," "us," or "our") respects the intellectual property rights of others and expects its users to do the same. In accordance with the Digital Millennium Copyright Act of 1998 ("DMCA"), the text of which may be found on the U.S. Copyright Office website at <https://copyright.gov>, we will respond expeditiously to claims of copyright infringement committed using our online platform, service, or website (collectively, the "Service").

Please note that our Service operates as an aggregator of third-party artificial intelligence (AI) models. Outputs are generated automatically by third-party technology in response to user-submitted prompts and files. If you believe that any content hosted on or generated through our Service infringes your copyright, please follow the procedures outlined below.

1. DESIGNATED COPYRIGHT AGENT

The Company's Designated Copyright Agent to receive notifications of claimed infringement is:

- **Attn:** Copyright Agent / Legal Department
- **Company Name:** IQBID Helios Limited
- **Corporate Address:**
- **Email Address:** dmca@iqbid.ai
- **Telephone:**

For a notice to be effective under the DMCA, it must be sent to the Designated Copyright Agent listed above via email or written communication.

2. NOTIFICATION OF COPYRIGHT INFRINGEMENT (TAKEDOWN NOTICE)

If you are a copyright owner, authorized to act on behalf of one, or authorized to act under any exclusive right under copyright, please report alleged copyright infringements taking place on or through the Service by submitting a written DMCA Notice containing the following information:

1. **Identification of the copyrighted work** that you claim has been infringed, or, if multiple copyrighted works are covered by a single notification, a representative list of such works.
2. **Identification of the material or output** that you claim is infringing (or to be the subject of infringing activity) and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material (including the specific URL link, screenshot, and/or prompt details).
3. **Information reasonably sufficient to permit us to contact you**, such as your physical address, telephone number, and, if available, an email address.
4. **A statement that you have a good faith belief** that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
5. **A statement that the information in the notification is accurate**, and under penalty of perjury, that you are the copyright owner or authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
6. **A physical or electronic signature** of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Failure to include all of the above information may result in a delay or rejection of your DMCA notice.

3. HOW WE PROCESS TAKEDOWN NOTICES

Upon receipt of a valid and complete DMCA Notice, Company will take the following steps:

- Expeditiously remove or disable access to the allegedly infringing material.
- Notify the user who submitted the prompt/file or generated the output that we have removed or disabled access to the material.
- Log the incident as part of our Repeat Infringer Policy.

4. COUNTER-NOTIFICATION PROCEDURES

If you receive a notification from us that content generated or uploaded by you has been removed due to a copyright infringement claim, and you believe this occurred by mistake or misidentification, you may elect to file a Counter-Notice.

To be effective, a Counter-Notice must be a written communication sent to our Designated Copyright Agent that includes substantially the following:

1. **Identification of the material** that has been removed or to be disabled and the location at which the material appeared before it was removed or disabled.
2. **A statement under penalty of perjury** that you have a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.
3. **Your name, address, telephone number, and email address.**
4. **A statement that you consent to the jurisdiction** of the Federal District Court for the judicial district in which your address is located (or, if your address is outside of the United

States, that you consent to the jurisdiction of any United States Federal District Court where the Company may be found), and that you will accept service of process from the person who provided the original DMCA notification or an agent of such person.

5. Your physical or electronic signature.

Upon receipt of a valid Counter-Notice, we will forward it to the original complaining party. If the copyright owner does not file a court action seeking a court order against you within ten (10) to fourteen (14) business days, we are permitted by law to restore the removed material or cease disabling access to it.

5. REPEAT INFRINGER POLICY

In accordance with the DMCA and other applicable laws, Company has adopted a strict policy of terminating, in appropriate circumstances and at Company's sole discretion, users who are deemed to be repeat infringers. Company may also, at its sole discretion, limit access to the Service and/or terminate the accounts of any users who infringe any intellectual property rights of others, whether or not there is any repeat infringement.

6. IMPORTANT DISCLAIMER AND WARNING

UNDER SECTION 512(f) OF THE DMCA, ANY PERSON WHO KNOWINGLY MATERIALLY MISREPRESENTS THAT MATERIAL OR ACTIVITY IS INFRINGING MAY BE SUBJECT TO LIABILITY FOR DAMAGES, INCLUDING COSTS AND ATTORNEYS' FEES, INCURRED BY THE ALLEGED INFRINGER, BY ANY COPYRIGHT OWNER OR COPYRIGHT OWNER'S AUTHORIZED LICENSEE, OR BY US.

If you are unsure whether the material you are reporting is actually infringing, we strongly recommend contacting an attorney before filing a notice with us.

TERMS OF SERVICE — SECTION: FEES, SUBSCRIPTIONS AND BILLING, DISPUTE RESOLUTION AND ARBITRATION AGREEMENT

FEES, SUBSCRIPTIONS AND BILLING TERMS

1. Subscription Plans and Fees

By selecting a paid tier of the Service (a "Subscription Plan"), you agree to pay IQBID Helios Limited (the "Company") the recurring monthly or annual fees indicated for that Subscription Plan. All transactions for US users are processed by third-party providers of the Company's payment infrastructure, including Payment Systems. You authorize the Company and its payment systems to charge all applicable fees from the payment method you specify, including any taxes and transaction processing fees.

2. PRE-PAID ACCESS ONLY.

The Service operates strictly on a one-time, pre-paid basis. You purchase a specific volume of credits, prompts, or execution limits ("Credit Packs") for a designated timeframe. There are no recurring charges, subscription commitments, or automatic renewals. Once your purchased Credit Pack is exhausted, your access to advanced features will be suspended until you execute a new individual transaction. ALL PURCHASES ARE STRICTLY FINAL AND NON-REFUNDABLE."

3. Immediate Consumption of Digital Services

The Service provided constitutes the immediate provision of digital content, automated processing, and real-time access to aggregated third-party Artificial Intelligence (AI) models. By executing a transaction, you explicitly request and agree that the functional access to the Service, including your allocated prompt limits and token capacities, shall be delivered to your account immediately upon successful payment authorization.

4. Strict No-Refund and No-Credit Policy

EXCEPT AS EXPRESSLY PROVIDED IN THESE TERMS OR REQUIRED BY APPLICABLE LAW, ALL FEES AND CHARGES PAID TO THE COMPANY ARE STRICTLY NON-REFUNDABLE.

No refunds, partial credits, or pro-rated balances will be issued for:

- (a) Partially used subscription periods;
- (b) Unused prompt allocations, credits, or tokens within a billing cycle;
- (c) Your dissatisfaction with the automated stylistic outputs, accuracy, correctness, or temporary "hallucinations" of the aggregated third-party AI models;
- (d) Temporary downtime of individual third-party AI models (e.g., OpenAI, Google) that are beyond the Company's direct infrastructure control.

5. Usage-Based Limits (Tokens and Prompts)

Each Subscription Plan features specific quantitative usage limits (e.g., specific number of queries, processed files, or API tokens). Any unused allocations or balances at the conclusion of a monthly or annual billing period are strictly forfeited, do not roll over to the next billing cycle, possess zero cash value, and are completely non-redeemable for fiat currency, cryptocurrency, or credits.

6. Fraud Prevention and Chargeback Policy

The Company utilizes automated fraud detection mechanisms in conjunction with "Payment Processors". If you initiate an unauthorized or fraudulent chargeback, payment dispute, or reversal through your credit card issuer or bank for services already delivered, the Company reserves the absolute right to:

- (a) Immediately and permanently terminate your User Account and block your access to all infrastructure without prior notice;
- (b) Forfeit any remaining balances or content stored within your account; and
- (c) Report the fraudulent activity to global payment merchant networks and credit reporting agencies.

You agree to contact our billing support team at billing@iqbid.ai to resolve any billing discrepancies or errors before initiating any formal bank disputes.

GOVERNING LAW AND DISPUTE RESOLUTION (ARBITRATION AGREEMENT)

1. Mandatory Binding Individual Arbitration

PLEASE READ THIS SECTION CAREFULLY - IT MAY SIGNIFICANTLY AFFECT YOUR LEGAL RIGHTS, INCLUDING YOUR RIGHT TO FILE A LAWSUIT IN COURT.

You and IQBID Helios Limited (the "Company") agree that any dispute, claim, or controversy arising out of or relating to these Terms of Service, the Service, the breach, termination, enforcement, interpretation, or validity thereof, or the use of the Service (collectively, "Disputes") shall be resolved **EXCLUSIVELY BY BINDING, INDIVIDUAL ARBITRATION**, rather than in a court of general jurisdiction.

You and the Company explicitly waive the right to a trial by jury or to participate in a class action lawsuit.

2. Informal Dispute Resolution Required

Before initiating any formal arbitration proceedings, you and the Company agree to attempt to resolve the Dispute informally.

(a) To initiate this process, you must send a detailed written notice of your claim (a "Dispute Notice") to our legal department via email at legal@iqbid.ai.

(b) The Dispute Notice must contain your full name, registered email address, a description of the nature and basis of the claim, and the specific relief sought.

(c) You and the Company agree to negotiate in good faith to resolve the Dispute for a period of sixty (60) calendar days following receipt of the Dispute Notice. If the Dispute is not resolved within this sixty (60) day period, either party may proceed to file for formal arbitration.

3. Arbitration Rules and Forum

The arbitration shall be administered and conducted by the American Arbitration Association ("AAA") in accordance with its Consumer Arbitration Rules and/or Commercial Arbitration Rules, as applicable (the "AAA Rules"), except as modified by this Arbitration Agreement. The AAA Rules are available online at www.adr.org.

The arbitration proceedings shall be conducted entirely in the English language. Unless otherwise agreed between the parties, the arbitration shall take place remotely via

teleconference or video conference, or based solely on written submissions, to minimize costs for both parties.

4. Arbitrator's Authority and Decisions

The arbitration shall be presided over by a single, neutral arbitrator appointed in accordance with AAA rules. The arbitrator shall have the exclusive authority to resolve all disputes regarding the interpretation, applicability, enforceability, or formation of this Arbitration Agreement, including any claim that all or any part of these Terms is void or voidable.

The arbitrator's decision and award shall be final, binding, and non-appealable, and judgment on the award rendered by the arbitrator may be entered in any court having competent jurisdiction thereof. The arbitrator may award declaratory or injunctive relief only in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by that party's individual claim.

5. CLASS ACTION AND JURY TRIAL WAIVER

YOU AND THE COMPANY EXPLICITLY AGREE THAT EACH PARTY MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS, CONSOLIDATED, OR REPRESENTATIVE PROCEEDING.

Further, unless both you and the Company agree otherwise in writing, the arbitrator may not consolidate more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding.

6. Allocation of Arbitration Costs and Fees

Payment of all filing, administration, and arbitrator fees will be governed by the AAA's rules. For any individual, non-frivolous claim that does not exceed \$10,000 (USD), the Company agrees to pay its share of the AAA administrative fees, provided that you comply with the Informal Dispute Resolution procedure outlined in Section 2. Each party shall bear its own attorneys' fees and legal expenses unless the arbitrator determines that either the substance of the claim or the relief sought was frivolous or brought for an improper purpose (as measured by the standards set forth in Federal Rule of Civil Procedure 11(b)).

7. Opt-Out Procedure

You have the right to opt out of this Arbitration Agreement and the Class Action Waiver. To do so, you must send a clear, written opt-out notice via email to legal@iqbid.ai within thirty (30) calendar days from the date you first register your User Account or access the Service.

Your opt-out email must include:

- (a) Your full legal name;**
- (b) Your registered account email address; and**
- (c) A unequivocal statement that you decline this Arbitration Agreement.**

If you opt out in compliance with this procedure, all other sections of these Terms of Service will continue to apply to you, and Disputes will be resolved in accordance with Section 8 below.

8. Governing Law and Venue for Non-Arbitrable Disputes

Except as otherwise required by applicable consumer protection laws, these Terms of Service, the Service, and any Disputes shall be governed by, and construed in accordance with, the laws of the Republic of Seychelles, without regard to its conflict of law principles.

In the event that this Arbitration Agreement is found to be unenforceable or if you successfully opt out under Section 7, you and the Company agree that any legal proceedings shall be brought exclusively in the competent courts located in Victoria, Mahé, Republic of Seychelles, and both parties hereby consent to the personal jurisdiction and venue of such courts.

US PRIVACY POLICY & STATE LAW DISCLOSURES

Effective Date: September 8, 2026

IQBID Helios Limited ("Company," "we," "us," or "our") respects your privacy and is committed to protecting your personal information. This Privacy Policy applies exclusively to users who reside in the United States of America ("US Users") and access or use our artificial intelligence (AI) model aggregation service, website, and related software applications (collectively, the "Service").

This Privacy Policy describes how we collect, use, disclose, retain, and protect your personal information, including specific disclosures required under state data privacy laws, such as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA"), and similar comprehensive state privacy frameworks.

1. INFORMATION WE COLLECT

In the preceding twelve (12) months, we have collected, and may continue to collect, the following categories of personal information from US Users:

- **Identifiers:** Name, email address, unique personal identifier, online identifier, Internet Protocol (IP) address, and account login credentials.
- **Commercial Information:** Records of Subscription Plans purchased, billing history, prompt credit usage, tokens consumed, and payment status (processed securely through third-party infrastructure providers such as "Payment Processors"). We do not store raw credit card numbers on our servers.
- **Internet or Other Electronic Network Activity:** Browsing history, search history, device type, operating system, and information regarding your interaction with our Service's user interface.
- **User-Generated AI Input Data:** The text prompts, inputs, queries, and any digital files (including images, documents, audio, or metadata) that you upload, submit, or transmit directly into the interface of our Service (collectively, "User Inputs").
- **AI-Generated Output Data:** Content automatically generated by third-party artificial intelligence models in response to your User Inputs (collectively, "Outputs").

2. HOW WE USE YOUR INFORMATION

We process and use the collected personal information for the following commercial and business purposes:

- **Service Delivery:** To provision your account, maintain your Subscription Plan, execute prompt requests, and route data seamlessly to aggregated third-party AI models.
- **Billing and Infrastructure Support:** To manage multi-currency recurring billing through "Payment Processors", process legitimate transactions, and mitigate transaction fraud.
- **AI Model Optimization and Training:** To analyze user engagement patterns, evaluate model performance, and actively train, retrain, or fine-tune our internal software, algorithmic routing matrices, and specialized AI models based on your User Inputs and generated Outputs.
- **Security and Compliance:** To enforce our Usage Policy, detect and prevent malicious or illegal activity, satisfy legal mandates, and defend against potential corporate liability or intellectual property claims.

3. HOW WE DISCLOSE AND SHARE YOUR INFORMATION

To deliver an aggregation service, your data must be transmitted to third parties. We do not sell your traditional personal identifiers (like your name or email) to data brokers. However, we disclose information under the following protocols:

- **Third-Party AI Infrastructure Providers (Sub-processors):** When you submit a prompt or file, it is automatically routed via API to independent AI infrastructure developers, including but not limited to OpenAI, LLC and Google LLC. These providers process data according to their commercial API enterprise agreements.
- **Payment Infrastructure Providers:** Financial logs and transactional identifiers are shared exclusively with "Payment Processors" and associated banking institutions to execute your Subscription Plan.
- **Legal Mandates:** We may disclose your information to federal or state law enforcement authorities if compelled by a valid legal subpoena, court order, or search warrant.

4. NOTICE OF AI DATA TRAINING AND USER OPT-OUT RIGHTS

As established in Section 2, the Company reserves the right to utilize anonymized or de-identified versions of your User Inputs (including uploaded files) and Outputs for the explicit purpose of machine learning optimization and AI model training.

YOUR PRIVACY CHOICES (OPT-OUT): If you prefer that your User Inputs and Outputs are not utilized by the Company for internal machine learning or algorithmic model training purposes, you possess the absolute right to opt out at any time. To exercise this right, you may:

1. Navigate to your Account Dashboard, select the "Your Privacy Choices" or "Data Control" tab, and toggle the switch to disable AI Model Training; or
2. Transmit an explicit written request via email to privacy@iqbid.ai stating your desire to restrict your inputs from model training activities.

Opting out of data training will not degrade your core user experience, reduce your prompt capacity, or impact your billing terms under your active Subscription Plan.

5. STATE-SPECIFIC PRIVACY RIGHTS (CCPA/CPRA DISCLOSURES)

If you are a resident of California (or states with equivalent privacy laws such as Virginia, Colorado, Connecticut, Utah, Texas, etc.), you possess specific statutory rights regarding your personal information:

- **Right to Know and Access:** The right to request that we disclose what personal information we collect, use, disclose, and sell about you over the past 12 months.
- **Right to Delete:** The right to request the deletion of your personal information collected or maintained by us, subject to specific regulatory exceptions (such as the necessity to maintain your active subscription or comply with financial record-keeping laws).
- **Right to Correct:** The right to request the rectification of inaccurate or outdated personal data stored within your account.
- **Right to Opt-Out of the "Sale" or "Sharing" of Data:** Under the broad statutory definitions of the CCPA, transferring user data to third-party AI models or utilizing files for machine learning might be interpreted as "sharing" data. You may restrict this via our "Your Privacy Choices" mechanism described in Section 4.
- **Right to Non-Discrimination:** We strictly prohibit any discriminatory pricing, latency degradation, or service denials against users who choose to assert their statutory privacy rights.

To submit a formal request to access, correct, or delete your data, please email our privacy compliance officer at privacy@iqbid.ai with the subject line "State Privacy Rights Request." We will verify your identity using your registered account email before executing any request.

6. DATA RETENTION POLICY

We retain your personal information, including historical billing records and login logs, for as long as your account remains active or as required to fulfill the business objectives outlined in this policy.

User Inputs (uploaded files and texts) and Outputs are securely cached on our infrastructure to maintain your session history. Cached files are retained for a standard period of ninety (90) calendar days from submission, after which they are systematically overwritten or completely de-identified for ongoing security analysis, unless an active user selects to delete their history manually at an earlier date.

7. THIRD-PARTY LINKS AND API REDIRECTIONS

Our Service bridges to third-party technology providers. Once your prompts and files are securely transmitted via API to third-party networks (OpenAI, Google, etc.), their downstream processing

becomes subject to their respective corporate privacy frameworks. We encourage you to review the developer terms of those individual AI model providers.

8. CONTACT INFORMATION

For any inquiries, structural clarifications, or data requests regarding this US Privacy Policy, please contact our legal and privacy infrastructure team at:

- **Email:** privacy@iqbid.ai
- **Attn:** Data Privacy Protection Officer
- **Corporate Address:**

CONSUMER HEALTH DATA PRIVACY POLICY

Effective Date: September 8, 2026

IQBID Helios Limited ("Company," "we," "us," or "our") issues this Consumer Health Data Privacy Policy to comply with applicable state privacy laws regulation-mandated in the United States, including the Washington My Health My Data Act ("MHMDA"), Nevada Senate Bill 370, and equivalent statutory frameworks.

This Policy applies exclusively to users residing in the United States ("US Users") who submit text prompts, structured queries, or digital files containing potential health-related information to our artificial intelligence (AI) model aggregation service (the "Service").

1. ABSOLUTE MEDICAL DISCLAIMER (NO MEDICAL ADVICE)

THE COMPANY IS A TECHNOLOGY SOFTWARE AGGREGATOR. THE COMPANY IS NOT A MEDICAL PROVIDER, HEALTHCARE INSTITUTION, OR LICENSED MEDICAL PROFESSIONAL.

THE SERVICE, INCLUDING ALL AUTOMATED OUTPUTS GENERATED BY THIRD-PARTY AI MODELS (E.G., OPENAI, GOOGLE), IS PROVIDED FOR GENERAL INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY. NO AUTOMATED OUTPUT CONSTITUTES, REPLACES, OR SHOULD BE INTERPRETED AS PROFESSIONAL MEDICAL ADVICE, DIAGNOSIS, CLINICAL INTERPRETATION, PROGNOSIS, OR TREATMENT. ALWAYS SEEK THE ADVICE OF YOUR PHYSICIAN OR OTHER QUALIFIED HEALTHCARE PROVIDER WITH ANY QUESTIONS YOU MAY HAVE REGARDING A MEDICAL CONDITION. NEVER DISREGARD PROFESSIONAL MEDICAL ADVICE OR DELAY IN SEEKING IT BECAUSE OF SOMETHING YOU HAVE READ ON OR GENERATED THROUGH THIS SERVICE.

2. CATEGORIES OF CONSUMER HEALTH DATA WE MAY PROCESS

Depending on how you interact with our aggregated AI models, you may voluntarily upload or input information that falls under the statutory definition of "Consumer Health Data" under US state laws. This includes:

- **Information Regarding Health Conditions:** Any text prompts describing physical or mental health conditions, clinical symptoms, diseases, syndromes, or medical histories.
- **Medical Diagnostic Documentation and Images:** Uploaded files, including but not limited to, photographs of dermatological conditions, digital copies of laboratory blood

tests, medical imaging data (X-rays, MRIs), or pharmaceutical prescriptions.

- **Biometric Data:** Facial features or physiological structures processed from uploaded photographic inputs by the third-party generative vision models.
- **Inferences:** Technical conclusions or structured summaries generated automatically by the aggregated AI models regarding your health baseline based on your submitted User Inputs.

3. PURPOSE OF PROCESSING AND LEGAL BASES

We collect, cache, and transmit Consumer Health Data strictly for the following operational reasons:

- **Real-Time Generation:** To forward your prompts and uploaded files via secure API to third-party AI models (Sub-processors) to execute the automated processing you explicitly request.
- **Temporary Session Caching:** To display your immediate historical workspace logs within your personal account dashboard.
- **Strict Security Auditing:** To evaluate whether submitted prompts violate our Usage Policy or contain prohibited materials.

CRITICAL POLICY ENFORCEMENT: UNLESS YOU PROVIDE SEPARATE, EXPLICIT, AFFIRMATIVE CONSENT, THE COMPANY STRICTLY PROHIBITS THE UTILIZATION OF CONFIRMED CONSUMER HEALTH DATA CATEGORIES FOR INTERNAL SOFTWARE TRAINING, MACHINE LEARNING, OR CORPORATE MODEL FINE-TUNING ACTIVITIES.

4. TRANSMISSION TO THIRD-PARTY SUB-PROCESSORS

To deliver our aggregation functionality, your submitted health-related data must be transmitted to third-party artificial intelligence infrastructure developers (such as OpenAI, LLC and Google LLC) via encrypted API channels. These third parties process data as independent infrastructure providers. We do not sell, rent, monetize, or lease your Consumer Health Data to commercial data brokers, marketing firms, or insurance agencies under any circumstances.

5. YOUR STATUTORY US PRIVACY RIGHTS

If you are a US resident, you possess distinct legal rights over your Consumer Health Data:

- **Right to Confirm Processing & Access:** The right to confirm whether we are processing health data about you and to obtain a list of all third-party sub-processors to whom your data has been transmitted via API.
- **Right to Delete:** The right to request the complete, permanent erasure of your cached personal health data and historical logs from our system and to compel our infrastructure providers to do the same.
- **Right to Withdraw Consent:** The right to immediately revoke any previous authorization regarding the processing or collection of your health data.

To exercise any of these statutory rights, you must submit a formal verification request via email to our dedicated data privacy department at privacy@iqbid.ai with the subject line "Consumer Health Data Request."

6. STATUTORY CONTACT AND DISCLOSURE REQUIREMENTS

This Consumer Health Data Privacy Policy is governed by the laws of the state jurisdiction of the consumer to the extent mandated by laws such as the Washington MHMDA. Any regulatory or consumer inquiries regarding our organizational data engineering pipelines can be submitted to:

- **Email Contact:** privacy@iqbid.ai
- **Attn:** Health Data Privacy Officer
- **Corporate Entity:**

ACCEPTABLE USAGE POLICY

Effective Date: September 8, 2026

This Acceptable Usage Policy ("AUP") defines the strictly prohibited activities and content restrictions governing your access to and use of the artificial intelligence (AI) model aggregation platform, website, and API infrastructure (collectively, the "Service") provided by IQBID Helios Limited ("Company," "we," "us," or "our").

This AUP is integrated directly into, and forms an inseparable part of, our United States Terms of Service. It applies to all users accessing the Service from the United States ("US Users"). Our Service routes data to third-party AI developers (including OpenAI, LLC and Google LLC). Consequently, you are strictly required to comply not only with our internal standards but also with the downstream enterprise usage terms mandated by those underlying AI infrastructure networks.

1. ABSOLUTE PROHIBITED CATEGORIES OF GENERATION AND CONTENT

You represent, warrant, and agree that you will not submit any text prompts, instructions, structured queries, or digital files (including documents, images, audio, or metadata) (collectively, "User Inputs"), or attempt to generate any machine learning outputs (collectively, "Outputs"), that fall within the following prohibited classifications:

A. Illegal Activity, Violence, and Physical Harm

- **Weapons and Explosives:** Developing instructions, blueprints, or operational guidance for fabricating, acquiring, or utilizing illegal firearms, ammunition, explosive devices, or chemical/biological weapons.
- **Incitement of Violence:** Generating content that incites, encourages, glorifies, or provides actionable instructions for committing acts of violence, self-harm, suicide, cyber-terrorism, or physical assault against individuals or groups.

B. Child Exploitation and Abuse Material (CSAM)

- **Absolute Zero-Tolerance:** Submitting, generating, hosting, or requesting any material related to Child Sexual Abuse Material (CSAM) or Child Sexual Exploitation and Abuse (CSAE). Any attempt to utilize our aggregated models to process, mutate, or render content involving minors in a sexually suggestive or exploitative context will result in immediate termination and federal law enforcement reporting.

C. Deception, Misrepresentation, and Political Fraud

- **Political Disinformation:** Utilizing generative text or vision models to execute coordinated influence operations, generate artificial political campaign materials, or create deepfakes of public officials, candidates, or private individuals without explicit statutory consent.
- **Plagiarism and Human Mimicry:** Misrepresenting AI-generated Outputs as being entirely authored or executed by a human being, particularly in academic, professional, legal, or journalistic environments where human authorship is a material requirement.
- **Impersonation:** Generating text, audio, or behavioral profiles to impersonate an actual physical individual or entity to commit financial wire fraud or identity theft.

D. Cybersecurity Threats and Malicious Code

- **Malware Engineering:** Directing AI models to write, debug, optimize, or reverse-engineer exploits, ransomware, spyware, Trojans, or payloads designed to compromise computing systems.
- **Social Engineering and Phishing:** Generating fraudulent emails, baiting scripts, spear-phishing materials, or deceptive landing page copy designed to extract credentials or sensitive financial data from consumers.

E. Financial and Medical Misrepresentation

- **Unlicensed Advisory:** Forcing models to generate definitive financial plans, speculative market trading buy/sell signals, legal contracts, or medical treatment regimens while falsely staging the output as licensed professional advice.

2. INFRASTRUCTURE PROTECTIONS AND REVERSE ENGINEERING

You are strictly prohibited from attempting to compromise the security, economic framework, or operational integrity of our Service. Prohibited actions include:

- **Jailbreaking and Prompt Injection:** Employing advanced semantic manipulation, adversarial inputs, or hidden code blocks designed to bypass the safety guidelines, moderation filters, or content restrictions of our Service or the underlying third-party APIs.
- **Scraping and Data Extraction:** Utilizing automated scrapers, bots, crawlers, or extraction tools to harvest synthetic training data, user histories, proprietary prompt matrices, or underlying model weights from our infrastructure.
- **Account Structuring:** Creating multiple duplicate accounts to evade subscription limits, abuse free tier prompt allocations, or obfuscate payment footprints monitored by Payment Processors.

3. REAL-TIME AI MODERATION AND COMPLIANCE MONITORING

To satisfy our statutory compliance duties and protect our enterprise API infrastructure:

- **Automated Screening:** Every User Input and generated Output is automatically processed through real-time, automated safety filters and classification models before being dispatched to downstream providers (OpenAI, Google, etc.).
- **Human Review:** The Company reserves the legal right to review historical system logs, chat records, and submitted files when an automated alert flags a high-probability violation of this AUP.

4. STRICT ENFORCEMENT, ACCOUNT SUSPENSION, AND FORFEITURE

If the Company, in its sole and absolute discretion, determines that you have violated any provision of this AUP, or that your interaction patterns pose an existential security or contractual ban risk to our enterprise API keys, we will execute immediate enforcement actions.

CONSEQUENCES OF VIOLATION:

1. **Immediate Account Termination:** Complete and permanent revocation of your access credentials, user profile, and cloud workspace without prior warning.
2. **Strict Financial Forfeiture:** All prepaid balances, remaining prompt quotas, token credits, and active subscription days under your current paid tier will be **permanently forfeited as a contractual penalty and are strictly non-refundable**.
3. **Legal Liability:** You agree to indemnify, defend, and hold harmless the Company against any third-party claims, regulatory enforcement penalties, or financial damages (including lost API access profits) resulting from your prohibited usage.