VELORA

International dating & paid-communication platform

AML / KYC & Content Moderation Policy

Prepared in response to acquirer / payment-service-provider due-diligence for high-risk dating (MCC 7273). Covers client verification, sanctions / PEP / adverse-media screening, ongoing monitoring, prohibited industries, and the content-moderation program.

Operating entity	[TO CONFIRM — legal entity name]
Registration / jurisdiction	[TO CONFIRM]
Policy owner (MLRO / Compliance)	[TO CONFIRM — name + email]
Version	v1.0
Effective date	[TO CONFIRM]
Classification	Confidential — for acquirer / scheme review

How to use this document

Items marked **[TO CONFIRM]** are commercial / legal facts only the operator can confirm (legal entity, signed vendor contracts, moderation headcount, MLRO appointment). Everything else is the operating control the platform runs on. Section 9 records live-vs-pending implementation status so nothing is misrepresented to a bank or scheme.

EXECUTIVE SUMMARY

0. Direct answers to the due-diligence questions

(A) Systems / vendors for client verification (PEP, sanctions, adverse media) under KYC, due diligence & ongoing monitoring

Purpose	Vendor	Used for
Identity + age (18+) verification, liveness / selfie	Sumsub (or Onfido / AU10TIX / Veriff)	Government-ID + selfie liveness at onboarding; documentary age proof
Selfie / photo & content risk scoring	HIVE (hive.com)	Automated check of the registration selfie and all uploaded media
Sanctions, PEP & adverse-media screening + ongoing monitoring	ComplyAdvantage	Screen every registrant and payer against OFAC / UK OFSI / EU / UN sanctions, PEP and adverse-media lists; continuous re-screening
Crypto exposure (if crypto rails used)	Elliptic	Wallet screening / source-of-funds
Chargeback & dispute intelligence	Ethoca + Verifi (CDRN / RDR)	Pre-dispute alerts, deflection, evidence collection
Text / image AI content scanning	HIVE + OpenAI moderation (via G2 LLC / OpenAI Global LLC)	Detect nudity / adult, CSAM, violence / terror, escort and other prohibited content in profiles and chat
CSAM hash-matching & reporting	PhotoDNA + NCMEC pipeline	Zero-tolerance detection and mandatory reporting of child sexual abuse material

Onboarding flow: after registration and selfie submission, the platform runs the user through HIVE + the identity-verification vendor. **Until verification completes the user is invisible and cannot contact anyone.** If any trigger fires, a compliance employee contacts the user for additional information and may block the account.

(B) Prohibited-industries / prohibited-activities policy — YES

The Company maintains a written Prohibited Content & Activities policy (Section 6, mirrored in the public Terms of Use §3 / §5). It bars escort / prostitution / sexual services for money, adult / pornographic content, CSAM, human trafficking, sanctioned-party dealings, weapons / drugs solicitation, fraud / scam and off-platform money movement. Users are contractually barred and are removed on detection.

(C) Content control & monitoring — layered program

Every profile, photo, video and message is screened by automated AI classifiers (HIVE + OpenAI) for nudity / adult / CSAM / copyright / prohibited content, backed by a human moderation team (**[TO CONFIRM headcount — e.g. ~40 FTE]**), an in-product user reporting mechanism, fake / AI-avatar profile detection, duplicate-registration control (one account per person), and a documented step-by-step moderation flow. CSAM is hash-matched and reported to NCMEC.

1. Purpose & scope

This policy sets out how Velora prevents money laundering, terrorist financing, sanctions breaches, fraud and the publication of prohibited content, in line with its acquiring bank(s), the card schemes (Visa high-risk / Integrity Risk Program (VIRP); Mastercard BRAM), and applicable AML law in the operating jurisdiction. It applies to all users, staff and moderators, and every payment, messaging and content surface.

Velora is a paid-communication dating platform: users buy credits and spend them on messages, letters, gifts, video and contact reveals. It is **not** an escort, adult, or sexual-services marketplace, and such use is prohibited (Section 6).

2. Customer onboarding & KYC

2.1 Age verification — strictly 18+

- Hard 18+ age gate at registration; date of birth captured and validated.
- Documentary age / identity proof via the IDV vendor (government ID + selfie liveness) is required before a user becomes visible or can communicate.
- Any user who cannot prove they are 18+ is refused and blocked; suspected minors are removed immediately and, where CSAM is involved, reported (2.4 / 4.4).

2.2 Identity & selfie verification flow

- User registers (name, email, DOB) and submits a selfie.
- The selfie + any uploaded media are checked by HIVE; identity is verified by the IDV vendor (ID + liveness).
- Until verification completes the user is invisible and cannot contact other users.
- If any trigger arises (mismatch, suspected minor, prohibited content, sanctions / PEP hit), a compliance employee contacts the user and may block the account.

2.3 Sanctions, PEP & adverse-media screening

- Every registrant and every payer is screened by ComplyAdvantage against global sanctions (OFAC, UK OFSI, EU, UN, HMT), PEP and adverse-media lists.
- **Russia & Belarus exclusion:** the Company operates no business, users, staff, payments or infrastructure connections with Russia or Belarus. Registrations, cards / BINs and IPs tied to these jurisdictions are blocked.
- Positive / possible matches route to manual review before the account can transact.

2.4 Ongoing monitoring & due diligence

- Continuous re-screening of the customer base against updated sanctions / PEP / adverse-media.
- Transaction monitoring for structuring, velocity, high-value top-ups, mismatched geo / BIN, and unusual spend.
- Enhanced Due Diligence (EDD) for high-risk indicators: source-of-funds questions and senior-compliance sign-off.
- Record-keeping of verification, screening and monitoring evidence for [TO CONFIRM — e.g. 5 years] after the relationship ends.

3. Fraud, chargeback & scam monitoring

3.1 Account & payment abuse controls

- **One account per person** — duplicate-registration control via device / email / BIN / behavioural signals; second accounts are blocked.
- Banning is enforced by linking email + profile name; for transactions, blocking is applied by BIN (Bank Identification Number).
- Card / payment fraud controls: 3-D Secure, velocity limits, a hard cap on a single top-up, and BIN / geo risk rules.

3.2 Chargebacks (CHB)

- Users contact the Client Care Centre for chargeback issues, where documents and information are collected.
- Third-party services Ethoca, Verifi and ComplyAdvantage manage CHB situations (pre-dispute alerts, deflection, evidence, AML checks).
- Chargeback ratios are actively managed within Visa VDMP / Mastercard ECM limits.

3.3 Fake profiles & AI-generated avatars

- Fake-profile / AI-avatar detection: uploaded photos are screened for AI-generated / synthetic imagery and reuse of stock / celebrity images; suspected fakes are held for review and removed if confirmed.
- Anti-catfishing / romance-scam controls: pattern detection for off-platform money requests, gift-card / crypto solicitation and scripted scam language.

3.4 Reporting mechanism

Every profile and every message carries a user “Report” control. Reports are triaged by the moderation team and can trigger takedown, account block, refund / CHB handling and, where required, law-enforcement referral.

4. Content moderation program

4.1 Layered moderation

- **Automated AI screening (first line):** all profiles, photos, videos and chat are scanned by HIVE and OpenAI moderation (via G2 LLC / OpenAI Global LLC) for nudity / adult, CSAM, violence / terror, escort / solicitation, hate, self-harm and copyright-infringing content.
- **Human moderation (second line):** a dedicated team of [TO CONFIRM ~ headcount, e.g. ~40 FTE] reviews AI alerts, streams / live content and edge cases.
- **User reporting (third line):** in-product reporting escalates content / behaviour to the team.

4.2 What is screened & blocked

- No adult / pornographic content anywhere on the platform (profiles, media, chat, video).
- Text filtering for terrorism / extremism and for scam / fraud language (off-platform money, bank details, gift-card / crypto requests).
- Visual screening of every photo / video for nudity, adult, and copyright-infringing content before it is shown.
- Escort / prostitution, politically provocative / illegal content, drugs / weapons solicitation.

4.3 Moderation flow (step-by-step)

- Content submitted → auto-scan (HIVE / OpenAI).
- Clean → published. Flagged → quarantined (not publicly visible) pending review.
- Human moderator reviews the alert within [TO CONFIRM SLA].
- Action: approve / edit-request / remove / warn / suspend / permanently ban (email + profile-name link; BIN block for payment abuse).
- Escalation: CSAM → 4.4; sanctions / AML → MLRO; fraud → risk team + CHB vendors.
- Audit: every decision logged with reviewer, timestamp, reason and evidence.

4.4 CSAM — zero tolerance

Any suspected child sexual abuse material is hash-matched (PhotoDNA), the account frozen, content preserved, and a report filed with NCMEC (and local authorities as required). No warning to the user.

5. Governance, roles & training

- MLRO / Compliance Officer [TO CONFIRM] owns AML / KYC, sanctions and SAR / STR reporting.
- Trust & Safety / Moderation lead owns the content program.
- Staff and moderators receive AML, sanctions, CSAM-handling and content-policy training at onboarding and at least annually.
- Suspicious Activity Reports (SAR / STR) are filed to the relevant FIU where thresholds / indicators are met; tipping-off is prohibited.

6. Prohibited content & activities

Mirrors public Terms of Use §3 (Acceptable Use) and §5 (Prohibited Content & Activities). The following are strictly prohibited and cause content removal and / or permanent ban:

- Under-18 use or any content involving minors; CSAM (reported to authorities).
- Escort, prostitution, or any sexual service for money; solicitation of the same.
- Adult / pornographic / nudity content of any kind.
- Fraud, scams, romance fraud, phishing, or requests to move money off-platform (bank transfer, gift cards, crypto, wire).
- Human trafficking, exploitation, coercion.
- Sanctioned-party dealings; any Russia / Belarus nexus.
- Weapons, drugs, illegal-goods solicitation.
- Hate, harassment, violence, terrorism / extremism, self-harm promotion.
- Impersonation, fake / AI-generated identities, catfishing, duplicate accounts.
- Copyright / IP-infringing media.
- Money laundering / terrorist financing in any form.

The Company reserves the right to remove content, suspend or permanently ban users, withhold or refund funds, block by BIN, and report to schemes / law enforcement.

7. Payments & card-scheme (high-risk) compliance

- Merchant category: dating (MCC 7273) — treated as high-risk; the Company expects registration in Visa's high-risk / Integrity Risk Program (VIRP) with enhanced monitoring, and Mastercard BRAM compliance. [TO CONFIRM acquirer registration]
- Clear billing descriptor, transparent credit pricing (no subscriptions / hidden renewals), visible refund / cancellation terms, and accessible customer support — all live on the marketing / legal pages.
- No prohibited MCC blending — the platform sells only dating credits; no adult / escort MCCs.
- Dispute ratios monitored against VDMP / ECM; CHB tooling per 3.2.

8. Data protection & retention

- Personal and verification data is processed lawfully, stored securely, and retained only as long as required for compliance and legal obligation.
- Users are anonymous to one another until they choose to exchange contact details through the contact-request process.
- Payment data is handled by PCI-DSS-compliant processors; the platform does not store full card numbers.

9. Implementation status (operator honesty note)

Live vs pending

Live in the product today: 18+ gate, profile review + ‘verified’ status, per-profile & per-message reporting, AI content-moderation pipeline (text + image) with quarantine, sanctions-geo (RU / BY) block, duplicate-account controls, credit-only (no-subscription) billing, refund & legal pages. **To be contractually onboarded before / at go-live** (so this policy is fully truthful for the acquirer): the named external vendors (IDV / HIVE / ComplyAdvantage / Ethoca / Verifi / PhotoDNA-NCMEC), the human moderation headcount, and the MLRO appointment. Replace every [TO CONFIRM] with the signed / appointed fact before submission — do not represent a control as live to a bank / scheme until it is.

The public-facing subset of this policy lives in Velora’s Terms of Use, Privacy Policy, Refund / Cancellation Policy and Anti-Scam Policy.