PROHIBITED CONTENT POLICY

SIA Synchron - shookout.com

Effective Date: 07.04.2026

Last Updated: 07.04.2026

1. INTRODUCTION

1.1 Purpose

This Prohibited Content Policy ("**Policy**") provides a comprehensive, detailed catalogue of content that is strictly prohibited on the shookout.com digital goods marketplace (the "**Platform**"), operated by SIA Synchron, registration number 40203436468, registered address Unijas iela 74A - 45, Riga, LV-1084, Latvia ("**Company**," "**we**," "**us**," or "**our**").

This Policy exists to: (a) provide Sellers, Buyers, moderators, and support personnel with a single authoritative reference for all content restrictions; (b) enable consistent, transparent, and proportionate enforcement decisions; (c) protect the Platform, its Users, and the public from illegal, harmful, and deceptive content; and (d) support Company's compliance with applicable law, including the EU Digital Services Act (Regulation (EU) 2022/2065, "**DSA**") and the EU AI Act (Regulation (EU) 2024/1689).

1.2 Scope

This Policy applies to all content uploaded, listed, submitted, communicated, or otherwise made available through the Platform, including: Digital Goods and their associated files; product listings, descriptions, titles, and tags; previews, thumbnails, screenshots, and samples; reviews, ratings, and comments; user profiles and profile content; messages and communications; and any other User Content.

1.3 Relationship to Other Documents

This Policy expands upon the prohibited content categories set forth in:

- Community Guidelines, Section 3 (Prohibited Content);
- Terms of Service, Section 9 (Prohibited Conduct and Content);
- Seller Agreement, Section 10 (Prohibited Conduct);
- Copyright & Takedown Policy, Sections 3-4 (IP notice-and-takedown and DSA notice-and-action).

Where this Policy provides greater specificity or additional examples compared to those documents, this Policy supplements them. The enforcement framework in Section 6

mirrors and references the graduated enforcement system in the Community Guidelines, Section 8, and the Seller Agreement, Section 11.

2. GENERAL PRINCIPLES

2.1 Content is prohibited if it: (a) is illegal under EU law, Latvian law, or the law of the jurisdiction from which it originates or to which it is directed; (b) violates the rights of third parties, including intellectual property rights, privacy rights, and rights to dignity; (c) is harmful, dangerous, or exploitative; (d) is deceptive, fraudulent, or misleading; (e) undermines the integrity, security, or trustworthiness of the Platform; or (f) violates any provision of this Policy, the Terms of Service, the Seller Agreement, or the Community Guidelines.

2.2 Where a category listed in this Policy includes the phrase "including but not limited to," the examples provided are illustrative and non-exhaustive. Content that falls within the spirit and purpose of a prohibition but is not specifically listed may still be removed or restricted.

2.3 The prohibitions in this Policy apply regardless of the artistic, creative, satirical, or educational intent claimed by the User, unless a specific exception is expressly stated (see Section 3.6.2 regarding artistic nudity).

3. STRICTLY PROHIBITED CONTENT

3.1 Child Sexual Abuse Material and Child Exploitation

Severity: ZERO TOLERANCE. Immediate permanent termination and law enforcement referral.

The following content is prohibited without exception:

(a) Any visual depiction (photograph, video, illustration, digital art, AI-generated image, or any other medium) of a minor engaged in sexually explicit conduct, as defined under Directive 2011/93/EU, 18 U.S.C. § 2256, and applicable national law;

(b) Any AI-generated, computer-generated, or digitally manipulated imagery depicting minors in sexual or exploitative contexts, regardless of whether the depicted minor is a real or fictitious person;

(c) Content that sexualises minors in any manner, including through suggestive poses, clothing, contexts, or accompanying text, even if the minor is not depicted in explicitly sexual conduct;

(d) Content that promotes, facilitates, instructs, or provides guidance for the grooming, exploitation, trafficking, or abuse of minors;

(e) Content that normalises or trivialises child sexual abuse;

(f) Any material that would constitute an offence under Directive 2011/93/EU on combating the sexual abuse and exploitation of children or under applicable national criminal law.

Enforcement: Content in this category is subject to immediate removal upon detection, permanent termination of all associated accounts, preservation of evidence, and mandatory reporting to: (i) the applicable law enforcement authority; (ii) the National Center for Missing & Exploited Children (NCMEC) under US law (18 U.S.C. § 2258A) where applicable; and (iii) the relevant national authority under Directive 2011/93/EU. No notice, warning, or appeal process applies prior to removal and account termination for this category.

3.2 Malware, Exploits, and Malicious Code

Severity: ZERO TOLERANCE for malicious intent. Nuanced treatment for legitimate security tools.

(a) Strictly Prohibited (no exceptions):

(i) Digital Goods containing viruses, worms, trojans, ransomware, spyware, adware, rootkits, keyloggers, backdoors, logic bombs, or any other code designed to damage, disrupt, surveil, or gain unauthorised access to any system, device, network, or data;

(ii) Cryptocurrency mining code embedded in Digital Goods without prominent disclosure and user consent;

(iii) Phone-home functionality, telemetry, or data exfiltration code hidden in Digital Goods without disclosure;

(iv) Code designed to disable, bypass, or circumvent security software, operating system protections, or digital rights management systems for unlawful purposes;

(v) Exploit kits, zero-day exploits, and tools designed primarily for launching cyberattacks against systems without authorisation;

(vi) Botnets, DDoS tools, credential stuffing tools, and brute-force attack tools;

(vii) Phishing kits, fake login page templates, social engineering toolkits, and any content designed to fraudulently obtain credentials, personal data, or financial information.

(b) Conditional Permission (legitimate security tools):

Security research tools, penetration testing frameworks, vulnerability scanners, and educational exploit demonstrations may be permitted where: (i) the Seller is a verifiable security professional or organisation; (ii) the listing clearly and prominently describes the tool as intended for authorised security testing only; (iii) the listing includes a disclaimer that unauthorised use is illegal; (iv) the tool does not target specific

production systems, services, or individuals; and (v) the tool complies with applicable law, including the EU Cybersecurity Act (Regulation (EU) 2019/881) and national computer crime legislation. Company reserves the right to require additional documentation or to restrict such listings at its discretion.

3.3 Pirated, Cracked, Nulled, and Counterfeit Content

Severity: HIGH. Content removal and repeat infringer policy applies.

(a) Software, plugins, themes, fonts, or other Digital Goods that have been cracked, nulled, patched, or otherwise modified to remove or circumvent licence validation, copy protection, or activation mechanisms;

(b) Unauthorised copies or redistributions of copyrighted works, including Digital Goods obtained from other marketplaces, subscription services, or creators without permission to resell;

(c) "Leaked" or pre-release content distributed without authorisation from the rights holder;

(d) Content marketed as "free download" or "nulled" versions of commercially licenced products;

(e) PLR (Private Label Rights) or MRR (Master Resale Rights) content where the upstream licence chain is broken, expired, or does not authorise the distribution model used on the Platform;

(f) Counterfeit or knock-off Digital Goods designed to imitate or pass off as the products of another creator or brand, including through confusingly similar naming, branding, or visual design;

(g) Digital Goods incorporating third-party assets (stock photos, fonts, icons, code libraries, UI kits) under licences that do not authorise redistribution or sublicensing to Platform Buyers;

(h) Bundles or compilations of third-party content aggregated without permission from each individual rights holder.

Cross-reference: Detailed IP rules and takedown procedures are set forth in the Copyright & Takedown Policy and the Community Guidelines, Section 4.

3.4 Fraud, Scams, and Deceptive Content

Severity: HIGH to ZERO TOLERANCE depending on intent and harm.

(a) Fraudulent Products:

(i) Digital Goods that serve no legitimate purpose and exist solely to extract payment from Buyers (e.g., empty archives, placeholder files with no actual content, password-locked files where the password is withheld);

(ii) Products marketed with fabricated testimonials, endorsements, certifications, or affiliations;

(iii) Products claiming to provide illegal benefits (e.g., "hack any account," "generate unlimited money," "bypass any paywall");

(iv) Fake licence keys, serial numbers, activation codes, or product keys for third-party software.

(b) Deceptive Listings:

(i) Listings where the product description, title, screenshots, or previews materially misrepresent the actual Digital Good delivered to the Buyer;

(ii) Bait-and-switch schemes: advertising one product but delivering a materially different or inferior product;

(iii) Hidden terms, conditions, or restrictions not disclosed in the listing that materially affect the Buyer's use of the Digital Good;

(iv) Artificially inflated file counts, page counts, asset counts, or feature lists that do not correspond to the actual content;

(v) Fake compatibility claims (e.g., claiming compatibility with software versions that the Digital Good does not support).

(c) Manipulative Practices:

(i) Fake scarcity or urgency tactics: false claims of limited availability, countdown timers, or "only X left" notices for unlimited digital products;

(ii) Fake reviews, ratings, and testimonials: fabricated, purchased, incentivised (without disclosure), or coordinated reviews, whether positive (self-promotion) or negative (competitor sabotage);

(iii) Ranking manipulation: artificial inflation of sales, views, favourites, or search rankings through fake accounts, bots, purchased traffic, or coordinated schemes;

(iv) Review extortion: threatening Sellers with negative reviews, or threatening Buyers to obtain positive reviews;

(v) Shill bidding or self-purchasing to inflate sales metrics.

(d) Financial Fraud:

(i) Products facilitating money laundering, tax evasion, or the concealment of criminal proceeds;

(ii) Pyramid schemes, Ponzi scheme templates, or multi-level marketing tools designed to defraud participants;

(iii) Counterfeit currency templates, fake financial instrument templates, or tools for creating forged financial documents;

(iv) Products designed to exploit payment systems, generate fraudulent chargebacks, or conduct payment card fraud.

3.5 Hateful, Violent, and Extremist Content

Severity: HIGH to ZERO TOLERANCE.

(a) Hate Speech:

Content that attacks, demeans, incites hostility toward, or advocates for discrimination against individuals or groups based on: race, ethnicity, or national origin; religion or belief; gender, gender identity, or gender expression; sexual orientation; disability; age; caste; immigration status; or any other characteristic protected under applicable law.

This includes: (i) content promoting ideologies of racial or ethnic supremacy; (ii) content denying, trivialising, or glorifying genocide, crimes against humanity, or war crimes; (iii) slurs, dehumanising language, or imagery targeting protected groups; and (iv) coded language, symbols, or imagery that, in context, constitute hate speech (e.g., established hate symbols, numeric codes associated with extremist movements).

(b) Incitement to Violence:

(i) Content that directly incites, encourages, or instructs specific acts of violence against individuals, groups, or property;

(ii) Content that glorifies, celebrates, or expresses support for acts of violence, including mass violence;

(iii) Threats of violence, whether conditional or unconditional, directed at individuals or groups.

(c) Terrorist and Violent Extremist Content:

(i) Content produced by, or on behalf of, organisations designated as terrorist organisations under EU, UN, US, or other applicable sanctions and counter-terrorism frameworks;

(ii) Content that recruits for, promotes membership in, or raises funds for terrorist or violent extremist organisations;

(iii) Instructional materials for committing acts of terrorism or violent extremism;

(iv) Propaganda and materials glorifying terrorist acts.

Cross-reference: Removal of terrorist content may be subject to Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, which may require removal within one hour of receipt of a removal order from a competent authority.

(d) Harassment and Threats:

(i) Content targeting specific individuals with threats, intimidation, or sustained harassment;

(ii) Doxxing: publishing or threatening to publish private personal information (address, phone number, workplace, family details) of individuals without consent;

(iii) Content intended to shame, humiliate, or harm the reputation of specific individuals through fabricated or misleading claims;

(iv) Stalking tools or content facilitating persistent unwanted contact.

3.6 Adult and Sexually Explicit Content

Severity: HIGH. Removal and potential account restriction.

3.6.1 Prohibited Adult Content:

(a) Pornographic material: content depicting sexual acts, genitalia, or sexual activity with a primary purpose of sexual arousal;

(b) Sexually explicit Digital Goods, templates, or tools (e.g., adult website templates with embedded pornographic content, sexually explicit AI prompts designed to generate pornographic output);

(c) Non-consensual intimate imagery (NCII): real or AI-generated intimate depictions of identifiable real persons without their verified consent, regardless of whether the imagery is distributed, sold, or offered free of charge;

(d) "Revenge porn" tools or templates designed to facilitate the non-consensual sharing of intimate imagery;

(e) Escort, prostitution, or sexual services advertising content;

(f) Content depicting or promoting sexual violence, coercion, or exploitation of any kind.

3.6.2 Exception for Artistic Nudity:

Content depicting nudity may be permitted where **all** of the following conditions are met: (i) the content has clear artistic, educational, medical, or professional merit (e.g.,

fine art, anatomy references for artists, medical illustration); (ii) the listing is accurately categorised and appropriately tagged using Platform content labels; (iii) the content does not depict or sexualise minors in any form; (iv) the content does not constitute NCII; and (v) the primary purpose of the listing is not sexual arousal. Company retains sole discretion to determine whether specific content qualifies for this exception.

3.7 Spam, Low-Quality, and Manipulative Listings

Severity: MODERATE. Warning and removal for first offences; escalation for patterns.

(a) **Mass Duplicate Uploads:** Uploading numerous identical or trivially differentiated Digital Goods (e.g., the same template with only colour or text variations) to flood categories or search results;

(b) **Keyword Stuffing:** Inserting irrelevant, misleading, or excessive keywords, tags, or phrases in titles, descriptions, or metadata to manipulate search visibility;

(c) **Empty or Placeholder Listings:** Listings without functional, complete Digital Goods, or with placeholder files intended to reserve positions in categories or search results;

(d) **Duplicate Listings:** Multiple active listings for the identical Digital Good from the same Seller, except where genuinely different licence tiers or bundles are offered;

(e) **Auto-Generated Listings:** Mass-produced listings created by automated tools without meaningful human quality review, resulting in low-quality, repetitive, or nonsensical content;

(f) **Off-Topic Content:** Digital Goods listed in categories that do not match their actual content or purpose;

(g) **Advertising and Promotional Spam:** Listings that exist primarily to advertise off-platform products, services, or websites rather than to sell a legitimate Digital Good.

3.8 Sanctions-Violating Content

Severity: ZERO TOLERANCE. Immediate removal, account termination, and potential law enforcement referral.

(a) Digital Goods or transactions involving individuals, entities, or jurisdictions subject to comprehensive economic sanctions under OFAC, EU Regulation 269/2014, UN Security Council resolutions, or Latvian national sanctions;

(b) Content originating from comprehensively sanctioned jurisdictions;

(c) Content that facilitates the evasion of sanctions, including tools for anonymisation, sanctions screening avoidance, or jurisdictional masking;

(d) Content that finances or materially supports sanctioned persons, entities, or activities.

Cross-reference: Terms of Service, Section 7; Seller Agreement, Section 9.

3.9 Privacy-Violating Content

Severity: HIGH.

(a) Databases, datasets, or compilations containing personal data of identifiable individuals collected, processed, or distributed without a valid legal basis under GDPR or other applicable data protection law;

(b) Tools designed for surveillance, tracking, or monitoring individuals without consent or lawful authority (e.g., spyware templates, GPS tracking tools, hidden camera solutions);

(c) Identity theft tools: templates or tools designed to create fake identity documents, impersonate individuals, or fraudulently obtain services in another person's name;

(d) Doxxing kits or compilations: aggregated personal information about specific individuals compiled for the purpose of harassment, intimidation, or harm;

(e) Deepfakes: AI-generated realistic depictions (image, video, audio) of identifiable real persons without their verified, documented consent, regardless of the purpose (see also Section 4.2);

(f) Facial recognition databases or tools designed for mass surveillance of individuals in public spaces without legal authority;

(g) Social engineering kits containing personal data harvested without consent.

3.10 Illegal and Regulated Products

Severity: HIGH to ZERO TOLERANCE.

(a) Content facilitating the sale, manufacture, or distribution of illegal drugs or controlled substances;

(b) Content facilitating the sale, manufacture, or distribution of weapons, firearms, ammunition, explosives, or components thereof where prohibited by applicable law;

(c) Content facilitating gambling where the Seller is not licenced to offer gambling services in the relevant jurisdiction;

(d) Content promoting or facilitating human trafficking or forced labour;

(e) Content that constitutes unauthorised practice of a regulated profession (e.g., legal templates marketed as legal advice, medical templates presented as medical diagnosis tools);

(f) Content that violates applicable consumer safety regulations.

4. AI-GENERATED CONTENT RESTRICTIONS

4.1 General AI Rules

All AI-generated content rules from the Community Guidelines, Section 5, and the Seller Agreement, Section 5, are incorporated by reference. The prohibitions below supplement those rules.

4.2 Prohibited AI-Generated Content

(a) **Deepfakes of real persons without consent:** AI-generated depictions (image, video, audio, voice clone) of identifiable real persons created without their verified, documented consent. This prohibition applies regardless of the purpose (commercial, satirical, political, or other);

(b) **Undisclosed AI content:** Any Digital Good that is substantially AI-generated or AI-assisted but is not labelled as such using the Platform's AI disclosure system. This includes deliberately misrepresenting AI-generated content as exclusively human-created, hand-drawn, hand-crafted, or similar;

(c) **AI content from unlawfully trained models:** Digital Goods generated by AI systems trained on datasets obtained through: unlawful scraping (in violation of robots.txt, platform terms of service, or applicable law); infringement of copyright opt-out mechanisms under Article 4 of the EU Copyright Directive (Directive 2019/790); or violation of data protection law (e.g., processing personal data in training sets without legal basis);

(d) **AI-generated CSAM:** Any AI-generated depiction of minors in sexual or exploitative contexts. Zero tolerance applies identically to Section 3.1;

(e) **AI systems for prohibited practices:** Content produced by or incorporating AI systems that engage in practices prohibited under Chapter II of the EU AI Act, including: subliminal manipulation techniques; exploitation of vulnerabilities of specific groups; social scoring by public authorities; and real-time remote biometric identification in publicly accessible spaces (except as permitted under the AI Act);

(f) **Deceptive synthetic media:** AI-generated text, images, audio, or video designed to mislead recipients into believing the content is authentic when it is not, including: fake news articles, fabricated scientific papers, counterfeit official documents, synthetic endorsements by real persons, and manipulated evidence;

(g) **Emotion manipulation AI:** AI-generated content designed to exploit psychological vulnerabilities, addictive patterns, or emotional distress for commercial gain.

4.3 Mandatory AI Disclosures

Failure to comply with the AI disclosure requirements set forth in the Seller Agreement, Section 5.2, constitutes a violation of this Policy. Required disclosures include: (a) AI-generated or AI-assisted label; (b) type of AI used; (c) extent of human involvement; (d) machine-readable metadata where feasible. See the Community Guidelines, Section 5, for the complete disclosure framework.

5. INTELLECTUAL PROPERTY VIOLATIONS

5.1 The following intellectual property violations are prohibited, as detailed in the Copyright & Takedown Policy and the Community Guidelines, Section 4:

(a) Copyright infringement: unauthorised reproduction, distribution, adaptation, or public communication of copyrighted works;

(b) Trademark infringement: unauthorised use of trademarks, service marks, or trade dress in a manner likely to cause confusion;

(c) Patent infringement: Digital Goods that embody or implement patented inventions without licence;

(d) Trade secret misappropriation: Digital Goods incorporating or derived from trade secrets obtained through improper means;

(e) Design right infringement: Digital Goods that copy registered or unregistered designs;

(f) Database right infringement: extraction or reutilisation of a substantial part of a protected database;

(g) Circumvention of technological protection measures (DRM circumvention) in violation of Article 6 of the EU Copyright Directive (Directive 2001/29/EC) or 17 U.S.C. § 1201.

5.2 Reports of IP infringement are handled through the procedures in the Copyright & Takedown Policy. The repeat infringer policy (three substantiated incidents in twelve months resulting in permanent termination) applies.

6. ENFORCEMENT AND CONSEQUENCES

6.1 Enforcement Framework

Enforcement follows the graduated system set forth in the Community Guidelines, Section 8, and the Seller Agreement, Section 11:

Level	Action	Applies to

Level 1: Warning	Written notice; 7-14 days to remediate	First-time minor violations (§3.7 spam, missing AI disclosure, listing inaccuracy)
Level 2: Content Removal	Listing removed with statement of reasons	Substantiated IP infringement, prohibited content, repeated quality violations
Level 3: Account Restriction	Feature limitations (listing creation, payouts)	Patterns of violations, refund rate thresholds
Level 4: Account Suspension	Full suspension, 30-180 days	Serious violations, repeated offences post-warning
Level 5: Permanent Termination	Account closed, 180-day payout hold, no new accounts	Zero-tolerance violations, 3+ IP strikes, fraud, illegal content

6.2 Zero-Tolerance Categories (Immediate Level 5)

The following categories result in immediate permanent termination without prior warning:

- Section 3.1: CSAM and child exploitation
- Section 3.2(a): Malware with malicious intent
- Section 3.4(d): Financial fraud (money laundering, counterfeit instruments)
- Section 3.5(c): Terrorist content
- Section 3.8: Sanctions violations
- Section 4.2(d): AI-generated CSAM

6.3 Statement of Reasons

In accordance with Article 17 DSA, every content moderation decision will be accompanied by a clear and specific statement of reasons, including: the provision of this Policy violated; the facts relied upon; information on automated means used (if any); and available redress mechanisms.

7. REPORTING PROHIBITED CONTENT

7.1 Any person may report content they believe violates this Policy:

- **Report Button**: available on every listing, review, and profile on the Platform;
- **Email (IP/Copyright)**: copyright@shookout.com;
- **Email (Other illegal content)**: report@shookout.com;
- **Email (CSAM / urgent)**: report@shookout.com (marked "URGENT: CSAM" in subject line).

7.2 Reports should include: (a) the URL of the content; (b) the category of violation (reference to this Policy where possible); (c) a description of the violation; and (d) the reporter's contact information (except for CSAM reports).

7.3 Detailed notice requirements for DMCA and DSA are set forth in the Copyright & Takedown Policy, Sections 3 and 4.

8. APPEALS

8.1 Users affected by enforcement decisions may appeal through:

- The "Appeal" button in the enforcement notification;
- Email to legal@shookout.com with subject "Appeal: [Reference Number]."

8.2 Appeals must be submitted within thirty (30) days (or six (6) months for DSA complaints) and must include: the decision being appealed, the grounds for appeal, and supporting evidence.

8.3 The full appeals process is described in the Community Guidelines, Section 10, and the Copyright & Takedown Policy, Section 6.

9. UPDATES TO THIS POLICY

Company may update this Policy to reflect changes in law, regulatory guidance, emerging threats, or Platform practices. Material changes will be communicated at least fifteen (15) days before the effective date via email and Platform notification.

10. CONTACT

Purpose	**Contact**
Report prohibited content	report@shookout.com or Report button
Copyright/IP reports	copyright@shookout.com
Appeals	legal@shookout.com

General support	support@shookout.com

SIA Synchron | Reg. No. 40203436468 | Unijas iela 74A - 45, Riga, LV-1084, Latvia