

Acceptable Use Policy

1. Overview

This Acceptable Use Policy (“AUP”) governs your access to and use of the AroFlo services (“Services”).

You must use the Services in compliance with all applicable laws, this AUP, the Terms and Conditions, the End-User Licence Agreement, and the Service Quotas & Usage Limits Policy.

You are responsible for all activity conducted under your account.

2. Prohibited Use

You may not use the Services to:

- (a) violate any applicable law or regulation;
- (b) infringe the rights of any third party, including intellectual property, privacy, or contractual rights;
- (c) upload, transmit, or distribute unlawful, harmful, fraudulent, or deceptive content;
- (d) interfere with or disrupt the integrity, performance, or security of the Services; or
- (e) use the Services in any manner inconsistent with their intended purpose.

3. Communications and Messaging

You must not use the Services to:

- (a) send unsolicited, bulk, or spam communications;
- (b) conduct marketing campaigns without appropriate consent;
- (c) generate excessive or abusive messaging traffic;
- (d) engage in phishing, spoofing, or deceptive communications; or
- (e) engage in activities that may harm email deliverability, third-party providers, or AroFlo’s reputation.

You are solely responsible for compliance with all applicable communications, anti-spam, and marketing laws.

4. AI and Machine Learning Use

You must not use AI-powered features to:

- (a) generate unlawful, harmful, misleading, or deceptive content;
- (b) produce high-volume or automated content outside intended workflows;
- (c) rely on AI outputs without appropriate human review where accuracy, safety, or compliance is required;
- (d) use AI outputs in high-risk or safety-critical scenarios without independent validation;
- (e) attempt to extract, reverse engineer, or replicate AI models or outputs; or
- (f) use AI functionality in a manner that creates excessive load or cost.

5. Automation, API, and System Use

You must not:

- (a) generate excessive or abusive API traffic;
- (b) bypass or attempt to bypass service quotas, rate limits, or system controls;
- (c) perform unauthorised load testing, stress testing, or benchmarking;
- (d) use automated systems that degrade platform performance; or
- (e) access or use the Services in a manner inconsistent with intended functionality.

6. Resource Usage and Quotas

You must not:

- (a) use the Services in a manner that materially exceeds normal usage patterns;
- (b) create excessive load that impacts system performance or other customers; or
- (c) attempt to circumvent any usage limits or billing controls.

All usage is subject to the Service Quotas & Usage Limits Policy here, as amended from time to time. Excessive or abusive usage may result in throttling, restriction, suspension, or additional charges.

7. Security and Integrity

You must not:

- (a) introduce malware, viruses, or harmful code;
- (b) attempt to gain unauthorised access to systems, accounts, or data;
- (c) probe, scan, or test vulnerabilities without authorization; or
- (d) interfere with or disrupt the operation of the Services or supporting infrastructure.

8. Data and Content Responsibilities

You are responsible for all data and content you submit, store, or process using the Services.

You must ensure that:

- (a) you have all necessary rights, consents, and permissions to use such data;
- (b) your data does not violate applicable laws or third-party rights;
- (c) you do not submit, store, or process prohibited or restricted data as described below; and
- (d) you do not use location-based features (including geofencing) without appropriate notice and consent where required by law.

Unless expressly agreed in writing by AroFlo, you must not use the Services to upload, store, process, or transmit:

- (a) Sensitive personal data, including:
 - * health or medical information;
 - * biometric identifiers (e.g. fingerprints, facial recognition data);
 - * genetic data;
 - * information about racial or ethnic origin, religious beliefs, or union membership;
- (b) Financial and payment data, including:
 - * credit or debit card numbers;
 - * bank account or routing numbers;
 - * payment authentication data (including PINs, CVV/CVC codes);
- (c) Government-issued identifiers, including:
 - * passport numbers;
 - * driver's licence numbers;
 - * national identification or social security numbers;
- (d) Highly sensitive authentication information, including:
 - * passwords (other than those managed through approved authentication mechanisms);



WorkLife, sorted.

* private encryption keys or API secrets;

(e) Data subject to heightened regulatory requirements, including:

* data subject to HIPAA, PCI-DSS, or similar regulatory frameworks, unless explicitly supported by the Services; or

(f) Any other data that would require AroFlo to implement additional compliance, security, or regulatory obligations not expressly agreed in writing.

If you submit prohibited data in violation of this section, you do so at your own risk.

AroFlo may remove, restrict, or delete such data without notice and may suspend or terminate access to the Services.

9. Enforcement

AroFlo may investigate any suspected violation of this AUP.

Where a violation is identified, AroFlo may, at its sole discretion and without liability:

- suspend or restrict access to the Services;
- throttle or block usage;
- remove or disable content;
- limit or disable specific features (including AI or email functionality);
- terminate accounts; or
- take any other action reasonably necessary to protect the Services or other users.

AroFlo may limit or withdraw access to support channels independently of access to the Services.

Enforcement actions may be applied without prior notice where reasonably necessary to protect AroFlo, its personnel, or other users.

10. Reporting Violations

You agree to promptly report any suspected misuse, security incident, or violation of this AUP.

11. Changes to this Policy

AroFlo may update this AUP from time to time.

Where changes are material, AroFlo will provide reasonable notice. Where changes are required to address security, legal, or misuse risks, updates may take effect immediately.

Continued use of the Services constitutes acceptance of the updated policy.

12. Acceptable Conduct and Interactions

You must interact with AroFlo personnel, including support, operations, and customer success teams, in a professional and respectful manner.

You must not:

- (a) engage in abusive, threatening, harassing, or discriminatory conduct;
- (b) use offensive, obscene, or inappropriate language;
- (c) engage in repeated, excessive, or unreasonable communications that disrupt or burden support operations;
- (d) submit malicious, bad faith, or intentionally misleading requests; or
- (e) engage in spamming, phishing, or other harmful communication practices.



WorkLife, sorted.

AroFlo may, at its sole discretion, restrict, suspend, or terminate access to the Services where your conduct towards AroFlo personnel is abusive, disruptive, or otherwise violates this section.

Such action may be taken immediately where necessary to protect AroFlo personnel or maintain service operations.

13. Relationship to Other Documents

This AUP forms part of your agreement with AroFlo and should be read together with:

- the Terms and Conditions;
- the End-User Licence Agreement;
- the AroFlo API Licence Agreement; and
- the Service Quotas & Usage Limits Policy.