

Acceptable Use Policy

Prohibited activities and required conduct for all users of the Jurion AI platform.

Document ID	JUR-LEG-005
Version	1.0
Effective date	2026-01-01
Last updated	2026-07-09
Category	agreements
Publisher	Jurion AI, jurion.uk

Subject to legal review

This document is provided for information only and remains draft until reviewed by a qualified solicitor. It does not constitute legal advice.

Jurion AI

info@jurion.uk
<https://jurion.uk>

Contents

1. Application	3
2. Prohibited activities	4
3. Enforcement	5
4. Reporting	6
5. General provisions and commercial protections	7
<i>Revision history</i>	9

1. Application

This policy applies to all Authorised Users of the Jurion AI platform and to any other person accessing the Service. Breach may result in suspension of access or termination in accordance with the Terms of Service.

2. Prohibited activities

2.1 Illegal use

Do not use the Service in a way that breaches applicable law, regulation or professional rules, or to facilitate any unlawful activity.

2.2 Abuse

Do not use the Service to harass, threaten, defame or intimidate any person, or to send content that is unlawful, harmful or offensive.

2.3 Reverse engineering

Do not decompile, disassemble or reverse engineer any part of the Service, except to the extent expressly permitted by applicable law that cannot be excluded by agreement.

2.4 Malware

Do not upload, transmit or distribute any file or content that contains viruses, trojans, worms, logic bombs or other malicious code.

2.5 Spam

Do not use the Service to send unsolicited bulk communications or communications that breach the Privacy and Electronic Communications Regulations or equivalent applicable law.

2.6 Credential sharing

Do not share Authorised User credentials with any other person. Each Authorised User account is personal to the individual named on it.

2.7 Security testing without permission

Do not perform penetration testing, vulnerability scanning, automated probing or other security testing against the Service without prior written authorisation from Jurion. Responsible disclosure of suspected vulnerabilities is welcomed under the Jurion AI Security Disclosure Policy.

2.8 Excessive automated use

Do not use the Service in a way that places an unreasonable load on the platform, that circumvents rate limits or entitlement controls, or that materially degrades the Service for other customers. Legitimate use of provided application programming interfaces within their documented limits is permitted.

3. Enforcement

Jurion may investigate suspected breaches of this policy and may suspend access or terminate the Service in accordance with the Terms of Service where a breach is confirmed. Where the breach relates to a specific Authorised User, Jurion may suspend that Authorised User pending review.

4. Reporting

Suspected breaches of this policy or of the security of the Service should be reported to security@jurion.uk.

5. General provisions and commercial protections

These general provisions apply to and form part of this document. Where a specific clause elsewhere in this document, in the Terms of Service or in the Data Processing Agreement addresses the same subject matter in greater detail, that more detailed clause prevails to the extent of any conflict.

5.1 AI limitations

Artificial intelligence features are assistive. Outputs are produced automatically and may contain errors, omissions, out-of-date information, inaccurate citations or content that is inappropriate for a specific matter. Jurion AI does not warrant that any AI output is accurate, complete, current or fit for any particular purpose and does not warrant that the Service is free from all errors or interruptions.

5.2 Human review requirement

Customer must ensure that a suitably qualified person reviews and approves any AI output before that output is relied on for legal advice, sent to a client, filed with a court or regulator, executed as a contract or used to make a decision that materially affects any person. Professional judgement of the reviewing individual remains authoritative.

5.3 Customer responsibility

Customer is responsible for its use of the Service, for the accuracy and lawfulness of the data it submits, for the actions of its authorised users and for compliance with applicable law and professional rules including where relevant the SRA Standards and Regulations. Customer must maintain appropriate matter management, supervision, conflict-checking and file-retention practices independently of the Service.

5.4 Acceptable use

Use of the Service is subject to the Jurion AI Acceptable Use Policy. Customer must not use the Service for unlawful purposes, to infringe the rights of any person, to attempt to circumvent the security of the Service, to submit content that is unlawful or that Customer does not have the right to submit, or in a way that materially degrades the Service for other customers.

5.5 Liability limits

Nothing in this document limits or excludes any liability that cannot be limited or excluded under applicable law, including liability for death or personal injury caused by negligence and for fraud. Subject to that, neither party is liable for indirect, incidental, consequential, special or exemplary damages, or for loss of profit, revenue, goodwill, anticipated savings, business opportunity or reputational loss, however arising.

Subject to the above, each party's total aggregate liability arising out of or in connection with this document in any twelve-month period will not exceed the fees paid by Customer to Jurion AI in that period. To the maximum extent permitted by law, the Service is provided "as is" and Jurion AI disclaims all warranties, whether express or implied, including any implied warranties of satisfactory quality, fitness for a particular purpose and non-infringement, other than those that cannot be excluded under applicable law.

5.6 Pilot status

Where the Service or a specific feature is provided on a pilot, beta, preview, evaluation or early-access basis, that Service or feature is provided "as is", may change or be withdrawn at any time and is not covered by the service-level commitments applicable to generally-available features. Pilot terms in the applicable order or the Pilot Programme Terms prevail over inconsistent provisions in this document.

5.7 Third-party services

The Service integrates with third-party services including cloud infrastructure, model providers, email providers, calendar providers and payment providers. Those third parties operate under their own terms and privacy notices. Jurion AI is not responsible for the availability, performance or acts and omissions

of third parties beyond its reasonable control, and Customer's use of any third-party service through the Service is subject to that third party's terms.

5.8 Data protection roles

Where Jurion AI processes personal data on behalf of Customer in connection with the Service, Customer is the controller and Jurion AI is the processor, and the Jurion AI Data Processing Agreement governs that processing. Where Jurion AI processes personal data as controller (for example account and billing data of authorised users and website analytics), the Jurion AI Privacy Policy governs that processing.

5.9 Service changes

Jurion AI may from time to time modify, add to or remove features of the Service in order to improve it, to reflect changes in third-party services, to reflect changes in law or regulatory guidance or to maintain security. Jurion AI will not make changes that materially reduce the overall functionality of the Service during a paid subscription term without giving reasonable prior notice.

5.10 Suspension rights

Jurion AI may suspend access to the Service or to specific authorised users, in whole or in part, where Jurion AI reasonably believes that continued access presents a security risk, that fees are materially overdue, that use of the Service is in material breach of this document or the Acceptable Use Policy, or that suspension is required by law or by a request from a competent authority. Where practicable Jurion AI will notify Customer before suspending access and will restore access as soon as the relevant circumstances have been resolved.

5.11 Security responsibilities

Jurion AI implements the technical and organisational security measures described in the Jurion AI Security Overview. Customer is responsible for configuring the Service in line with its own security requirements, for managing authorised user access including timely off-boarding, for enabling multi-factor authentication for its administrators, for protecting credentials and end-user devices, and for the security of any data that Customer chooses to export from the Service.

5.12 Draft status

This document remains draft and is subject to legal review until reviewed and approved by a qualified solicitor. It is provided for information only, does not constitute legal advice and should not be relied on as a final legal instrument until it has been so reviewed.

Revision history

Version	Date	Summary
1.0	2026-01-01	Initial published version.