COMPLETA

Completa Acceptable Use Policy

Version 1.0 · Published November 2026 · Effective 17 November 2026

Provided by B2wise Holdings Ltd, a company registered in England and Wales (company number 15488673), registered office 23 St. Johns, Enderby, Leicester, England, LE19 2BR ("Completa", "we"). Contact and formal notices: legalnotices@b2wise.com.

1 Permitted use

This Acceptable Use Policy (the "Policy") forms part of and is incorporated into the Completa Platform Terms of Service (the "Platform Terms"). Completa may update this Policy from time to time by publishing a revised version, subject to the notice provisions of the Platform Terms. A revised version applies from its stated effective date, and continued use of the Services after that date constitutes acceptance. Capitalised terms not defined in this Policy have the meanings given in the Platform Terms. Each customer organisation ("Customer") must ensure that its employees, contractors, builders, administrators, end users and any other person it authorises to access or use the Services (each, a "User") complies with this Policy, and is responsible for their acts and omissions as if they were the Customer's own. Customers and Users may use the Services only through authorised accounts, for lawful business purposes and in accordance with applicable documentation, subscription entitlements and law. They must provide accurate account information, safeguard credentials, use data, systems and integrations only with proper authority, and have all rights, lawful bases, notices and consents required for data and content they submit, access or process.

2 Prohibited activity

Customers and Users must not, and must not permit or assist any third party to: (a) upload, create, transmit, store or make available content that is unlawful, fraudulent, defamatory, threatening, harassing, exploitative, discriminatory, obscene, infringing, privacy-invasive or otherwise harmful, or that promotes illegal activity; (b) introduce malware or other harmful code, or conduct phishing, credential theft, spam, illegal surveillance or denial-of-service activity; (c) probe, scan, test or circumvent security, authentication, access controls, rate limits or technical restrictions except with Completa's prior written authorisation; (d) disrupt, overload, degrade or interfere with the Services or any network, system, account or data; (e) access, use or disclose any account, data, system or integration without authority, impersonate another person or misrepresent organisational authority; (f) infringe intellectual-property, confidentiality, privacy or other rights, or unlawfully process, scrape, harvest, re-identify or combine data; (g) submit special-category, criminal-offence, export-controlled or similarly regulated data unless expressly agreed and appropriately safeguarded; (h) extract, copy, reverse engineer, decompile, disassemble, derive or redistribute Completa's proprietary runtime, platform code or non-public technology, except to the minimum extent that such restriction is expressly prohibited by applicable mandatory law and only for the specific purpose permitted by that law; (i) evade metering, billing or usage limits, obtain allowances by artificial fragmentation or simulated

activity, or conceal production use; or (j) use automated means in a manner that imposes an unreasonable load, bypasses controls or facilitates any prohibited activity; or (k) engage in any other conduct that Completa reasonably determines is harmful to the Services, other customers, or Completa's legitimate business interests.

3 High-impact applications

Customers must not use the Services as the sole basis for decisions affecting safety, legal rights, access to essential services, finance, employment, healthcare or other similarly consequential matters. For any permitted high-impact application, the Customer must independently assess legality and risk, test and validate outputs, maintain appropriate human review and appeal safeguards, monitor performance and bias, and implement suitable security, accuracy, record-keeping and governance controls. The Customer is solely responsible for all outcomes arising from its high-impact use of the Services, and Completa shall have no liability in connection with any such use. The Services must not be used for emergency response, autonomous safety-critical operation or any use where failure could reasonably cause death, personal injury or material property or environmental damage, unless Completa has expressly agreed otherwise in writing. Completa may require further information, impose additional controls or refuse or discontinue any use case presenting unacceptable legal, security, safety or reputational risk.

4 Automated monitoring

Completa may use automated systems to detect anomalies including usage patterns, organisation relationships, user and email-domain indicators and unusual publishing behaviour. Automated outputs may inform, but do not limit, Completa's exercise of its enforcement rights under this Policy. Monitoring and retention will comply with the Privacy Notice and DPA.

5 Response and appeals

Completa may request explanations, restrict functionality, reverse abusive allowances, suspend users or organisations, or terminate for serious or repeated violations. Where practicable, Completa will endeavour to provide prior notice and an opportunity to respond, but shall not be obliged to do so; immediate protective action may be taken for urgent threats or where Completa reasonably considers delay would increase risk. Without prejudice to any other rights or remedies available to Completa, the Customer shall indemnify and hold harmless Completa against all losses, liabilities, costs (including reasonable legal costs), damages and expenses incurred by Completa arising out of or in connection with any breach of this Policy by the Customer or any of its Users, including costs of investigation, remediation and any third-party claims resulting from such breach.