

Oktopi Acceptable Use Policy 24th April 2026

This Acceptable Use Policy was last reviewed and updated on 24th April, 2026.

1 Introduction and scope

- (a) This Acceptable Use Policy (**Policy**) establishes the standards governing access to and use of Oktopi products and related services (**Services**) as provided from time to time by Oktopi Pty Ltd (**Oktopi**).
- (b) The Services may incorporate artificial intelligence functions or features (**AI Features**). This Policy also governs the use of any AI Features.
- (c) This Policy applies to all customers and any end users who access or use any of the Services (each a **User**).
- (d) By accessing or using the Services, each User agrees to be bound by, and to use the Services in compliance with, this Policy, and all applicable laws and regulations.

2 Prohibited Uses

Users must not access or use the Services in any manner that:

- (a) is contrary to any applicable law or regulation;
- (b) relates to, is in aid of, or comprises, any fraudulent activity;
- (c) is harmful to, discriminatory against, or otherwise violates the rights of, any individual, organisation or group of people;
- (d) infringes the intellectual property, privacy, moral or other legal rights of any third party;
- (e) promotes, facilitates or endorses violence or terrorism;
- (f) promotes, facilitates or endorses discrimination, exploitation or modern slavery;
- (g) involves the use or creation of any obscene, profane, indecent or otherwise objectionable material;
- (h) involves the use or creation of any content or activity that may be harmful to minors, or for any purposes related to any form of child exploitation or abuse;
- (i) involves deception, impersonation or misrepresentation, or is scam related;
- (j) interferes with the availability, integrity or security of the Services or any aspect of the technology or algorithms underpinning the Services;
- (k) involves reverse engineering, decompiling, or otherwise attempting to derive the source code of any aspect of the technology or any algorithms underpinning the Services, or is directed towards designing, developing or building any algorithms, code or technology which replicates or is substantially comparable to the Services; or

- (l) involves the creation or distribution of any malicious code, spam or unsolicited communications.

3 AI Features

- (a) Without limiting the Users' obligations in section 2 above, Users must use any AI Features responsibly, lawfully and otherwise in accordance with this section 3.
- (b) Users must not use AI Features:
 - (1) to generate and rely on, or provide to a third party, any information or advice that would ordinarily be provided by a licensed professional (including, without limitation, medical, legal or financial advice), and for the avoidance of doubt, any outputs do not constitute such professional advice;
 - (2) to make, implement or activate any automated decisions or decision making that has or may have a material impact on an individual's or entity's legal position or similar significant effect without adequate human oversight;
 - (3) to explicitly predict or categorise individuals based on protected characteristics (including, without limitation, race, origin, ethnicity, political opinions, religious beliefs, gender, sexual orientation, age, disability, health status, or criminal history);
 - (4) to collect, analyse, or categorise biometric identifiers (including, without limitation, facial geometry, voiceprints or iris scans) without consent, or to build facial recognition databases;
 - (5) to input, upload, submit or otherwise process any patient level data, individual patient records, or any personal or health information that identifies or could reasonably identify a specific patient or research participant, whether directly or in combination with other information;
 - (6) to engage in plagiarism or academic dishonesty; or
 - (7) in relation to the development, control or use of weapons, explosives, or other materials capable of causing mass harm.

4 Security and responsibility

- (a) Users are responsible for maintaining the security of their accounts and credentials (eg usernames and passwords) and must not share their credentials with, or otherwise permit access to their account by, any third party.
- (b) Users must notify Oktopi immediately via email at support@oktopi.com if they suspect or discover any unauthorised access to or use of their accounts or the Services.

5 Investigation and enforcement

- (a) Oktopi may investigate any suspected breach of this Policy and may suspend or terminate access to the Services without prior notice where it considers necessary to do so.
- (b) A material breach of this Policy will be treated as a material breach of the customer's agreement with Oktopi.

6 Changes

Oktopi may update this Policy from time to time by posting a revised version on its website. By continuing to use the Services, Users agree to any revised or updated versions of this Policy.