



MJM TECHNOLOGY LTD

ACCEPTABLE USE POLICY

Version MJM-AUP-01 (v1.0) | Effective 21 September 2026 | www.mjm.technology/legal

IN PLAIN ENGLISH *The short version: use the services we provide for legitimate business purposes, don't do anything illegal or that puts security at risk, look after your passwords, and tell us straight away if you spot something suspicious. This policy is part of your agreement with us — no separate signature needed.*

This Acceptable Use Policy (“AUP”) applies to all customers of MJM Technology Ltd and governs the use of IT systems, networks, cloud services, equipment, and any other technology services (collectively, “Services”) provided by MJM Technology. By using the Services, the Customer and its users agree to comply with this AUP. This AUP is incorporated into and forms part of the MJM Technology Customer Terms and Conditions (MJM-TC-01).

1. Permitted Use

The Services may only be used for lawful purposes in connection with the Customer’s legitimate business activities. Users must comply with all applicable laws, regulations, and codes of practice, including the Computer Misuse Act 1990, the Communications Act 2003, and the UK General Data Protection Regulation.

2. Prohibited Activities

IN PLAIN ENGLISH *In short: nothing illegal, no hacking, no malware, no phishing or spam, no disabling security controls, no security testing without written sign-off, and no reselling our services without permission.*

The following activities are strictly prohibited. Users must not use the Services to:

- access, transmit, distribute, or store content that is illegal, defamatory, obscene, discriminatory, or that incites violence or hatred;
- gain or attempt to gain unauthorised access to any computer system, network, or data, including systems managed by MJM Technology or third parties;
- introduce, distribute, or execute malware, viruses, ransomware, spyware, or any other malicious code;
- conduct, facilitate, or participate in phishing, social engineering, spam, or any form of fraudulent communication;
- deliberately circumvent or disable security controls, firewalls, authentication mechanisms, or audit logs;
- conduct denial-of-service attacks, port scanning, or any form of network disruption;
- use automated tools to harvest data, credentials, or system information without prior written authorisation;
- perform penetration testing, vulnerability scanning, or offensive security activities against any systems (including Customer systems) without a written Penetration Testing Authorisation Letter from MJM Technology;
- copy, transmit, or disclose MJM Technology’s or any third party’s confidential or proprietary information without authorisation;
- use the Services in a manner that breaches any third-party rights, including intellectual property rights or rights of privacy;
- engage in cryptocurrency mining, illegal file sharing, or any activity that consumes excessive bandwidth or resources; or
- resell, sub-licence, or otherwise make the Services available to third parties without MJM Technology’s prior written consent.

3. Security Responsibilities

IN PLAIN ENGLISH *Keep passwords private, report anything suspicious quickly, keep unmanaged devices updated, and make sure visitors and contractors on your network follow these rules too.*

Customers and their users are responsible for:

- maintaining the security of their user credentials and ensuring that passwords are not shared;
- reporting any suspected security incident, unauthorised access, or vulnerability to MJM Technology promptly;
- keeping devices and software up to date where not covered by a managed service; and
- ensuring that third parties (including visitors and contractors) who access the Customer's network comply with this AUP.

4. Email and Internet Use

Where MJM Technology manages or provides access to email or internet services, users must not:

- send unsolicited bulk email (spam) or use email to harass, intimidate, or impersonate others;
- open email attachments or click links from unknown or suspicious sources; or
- send or receive material that is illegal, inappropriate, or in breach of section 2 above.

5. Consequences of Breach

IN PLAIN ENGLISH *Breaking this policy is treated as a serious breach of your contract. Depending on severity, we may suspend services, end the agreement, involve the authorities, or recover costs.*

Breach of this AUP constitutes a material breach of the Agreement between the Customer and MJM Technology. MJM Technology reserves the right to: (a) immediately suspend or restrict access to the Services; (b) terminate the Agreement in accordance with the Customer Terms and Conditions; (c) report the matter to relevant law enforcement or regulatory authorities; and (d) seek damages and costs arising from the breach.

6. Changes to this Policy

IN PLAIN ENGLISH *We can update this policy as the law, technology or our services change. If a change makes more work for you, we give you 30 days' notice first. Other changes take effect when we publish them.*

MJM Technology may update this AUP from time to time to reflect changes in the law, technology, or its services. The current version is published at www.mjm.technology/legal.

Where an update materially increases the Customer's obligations, MJM Technology shall give the Customer not less than thirty (30) days' prior written notice, in accordance with clause 15.4.1 of the Customer Terms and Conditions. Any other update takes effect on publication. Continued use of the Services after an update has taken effect constitutes acceptance of the revised policy.

7. Contact

If you have any questions about this AUP, or to report a suspected breach, please contact MJM Technology at security@mjm.technology or in writing to 101 Peckers Hill Road, St Helens, WA9 3JS.