



Acceptable Use Policy

Updated: 18 June 2026

Pennytel may update this document from time to time. The current version is published on our website.

Where a change materially affects your rights or obligations, we will provide any notice required by your agreement or applicable law.

1. Purpose and scope

This Acceptable Use Policy sets out how Pennytel services, networks, systems and websites may and may not be used.

It applies to:

- Pennytel customers;
- end users of Pennytel services; and
- any person who uses Pennytel services with a customer's authority.

Customers are responsible for ensuring that all authorised users of their Pennytel services comply with this policy.

In this policy, **Services** includes Pennytel mobile, internet, voice, VoIP, SIP, PBX, messaging and related telecommunications services, together with any associated systems, networks, portals and websites made available by Pennytel.

2. Lawful, responsible and non-harmful use

You must use the Services only for lawful purposes and in a way that does not harm Pennytel, our suppliers, our customers or other users of telecommunications networks or the internet.

You must not use, or allow the Services to be used:

- in breach of any law, regulation, code, standard or lawful direction;
- to engage in fraud, deception, scams or other unlawful activity;
- to infringe another person's intellectual property, privacy or other legal rights;
- to threaten, harass, abuse, intimidate or unlawfully discriminate against another person;
- to transmit, store, publish or distribute unlawful material; or
- to transmit, distribute or make available viruses, malware, ransomware, spyware, worms, trojans or other harmful software or code.

3. Messaging, spam and electronic marketing

You must not use, or allow the Services to be used, to send, facilitate or support spam, scam messages or other unlawful electronic messages.

When using the Services to send, facilitate, support, access, operate, administer or control emails, SMS, MMS, instant messages or other electronic messages, you must comply with the Spam Act 2003 and all other applicable laws, regulations, codes, standards and lawful directions.

This includes ensuring that commercial electronic messages are sent lawfully, identify the sender where required, and include a functional unsubscribe facility where required.

This section applies whether messages are sent directly using a Pennytel Service or indirectly using a third-party platform, application, gateway, messaging provider, CPaaS provider, marketing automation platform or similar service accessed through a Pennytel Service, including by using mobile data supplied by Pennytel.

You must not use, or allow the Services to be used:

- to send unsolicited commercial electronic messages in breach of applicable law;
- to send bulk messages unlawfully;
- to use, acquire, supply or facilitate the use of address-harvesting software or harvested-address lists;
- to host or operate websites, reply-to addresses or other facilities used to support spam activity;
- to collect or harvest email addresses, mobile numbers or other contact details for unlawful messaging purposes;
- to send, originate, relay, facilitate, support, access, operate, administer or control any SMS, MMS, electronic messaging, application-to-person messaging, CPaaS, marketing automation, messaging gateway or similar platform or service in a way that breaches, or may cause Pennytel or its suppliers to breach, any applicable law, regulation, code, standard, scam-prevention requirement, spam-prevention requirement or sender identification requirement;
- to send or facilitate SMS or MMS messages using an alphanumeric sender ID, business name, brand name, trading name, sender name, message header or other sender identifier unless that sender identifier is registered, authorised and used in accordance with all applicable laws, regulatory requirements and industry standards;
- to use a sender ID, sender name, message header, calling line identification, number or other identifier that you are not authorised to use;
- to misrepresent, obscure, mask, spoof or falsify the identity of the sender of a message;
- to send or facilitate scam, phishing, impersonation, misleading, deceptive, fraudulent, unsolicited or unlawful messages; or
- to use a Pennytel Service as an access path, data connection, control channel or support service for any messaging platform, campaign or activity that would breach this policy if the messages were sent directly using a Pennytel Service.

Pennytel's supply of a mobile, internet, voice, VoIP, SIP, PBX, messaging or data service does not mean that Pennytel has approved, authorised, verified or registered any sender ID, messaging campaign, third-party messaging platform, message content, consent process or unsubscribe process.

Where Pennytel reasonably suspects that a Service is being used to send, facilitate, support, access, operate, administer or control SMS, MMS or other electronic messaging in breach of this policy, Pennytel may require you to provide reasonable information or evidence about that use.

This may include evidence of sender ID registration or authorisation, your authority to use a sender ID, the messaging provider used, the nature and purpose of the messages, consent records, unsubscribe processes, complaint handling processes, campaign volumes, message samples and any other information reasonably required to assess compliance.

If you do not provide information Pennytel reasonably requests, or if Pennytel reasonably believes the use may breach this policy, applicable law, an industry standard, a regulatory requirement or a supplier requirement, Pennytel may restrict, suspend, block, rate-limit or terminate the affected Service in accordance with this policy and your service agreement.

4. Network, system and security misuse

You must not use, or allow the Services to be used, to compromise, interfere with or undermine the security, integrity or performance of any network, system, service, device or account.

Prohibited conduct includes:

- accessing or attempting to access systems, accounts, data or services without authority;
- probing, scanning or testing the vulnerability of a system or network without proper authorisation;
- bypassing or attempting to bypass authentication, security or fraud-prevention controls;
- sending data that contains forged, invalid, misleading or deceptive headers, routing information, source information or addressing;
- relaying communications through third-party servers or systems without authority;
- overloading, flooding, mail bombing, crashing, disabling or otherwise interfering with a network, service or device;
- launching, participating in or facilitating denial-of-service or distributed denial-of-service attacks; or
- taking steps to obtain a service, feature, access right or benefit to which you are not entitled.

5. Voice, VoIP and telephony services

Pennytel supplies legitimate voice and VoIP services, including SIP trunks, hosted PBX, Teams Calling, inbound number services and other voice-related services.

- You must not use, or allow those Services to be used:
- to make, facilitate or support scam, fraudulent or unlawful calls;
- to manipulate, spoof, falsify or misrepresent caller identification or calling line information in a misleading or unauthorised way;
- to engage in toll fraud, international revenue-share fraud, artificial inflation of traffic or similar conduct;
- to bypass or attempt to bypass Pennytel's charging, routing, security, anti-fraud or usage controls;
- to exploit compromised PBX, SIP, voice or customer systems;
- to resell, wholesale, rebill or otherwise commercially supply Pennytel Services to third parties unless expressly permitted under your agreement with Pennytel; or
- in any other way that breaches applicable law, industry rules or your service agreement with Pennytel.

6. Mobile data, gateways and automated use

Unless expressly permitted under your agreement with Pennytel, you must not use, or allow a Service to be used:

- as part of a SIM box, GSM gateway, modem pool, automated messaging system, bulk messaging system, traffic-generation system or similar arrangement;
- to resell, rebill, wholesale, aggregate or commercially supply messaging, calling, data access or telecommunications capability to third parties;

- to generate artificial, abnormal, excessive, automated or non-human traffic;
- to bypass, avoid or undermine Pennytel's or its suppliers' routing, charging, security, fraud-prevention, spam-prevention, scam-prevention or sender identification controls; or
- to facilitate a telecommunications, messaging or platform service that has not been approved by Pennytel where approval is required under your agreement, this policy or applicable law.

7. Security of customer systems and devices

You must take reasonable steps to secure any systems, networks, devices, software and credentials used in connection with the Services.

This includes taking reasonable steps to:

- use appropriate passwords and access controls;
- protect systems and devices from malware and unauthorised access;
- maintain appropriate software, firmware and security updates;
- monitor and secure PBX, SIP, voice and other internet-connected systems where relevant; and
- act promptly where you become aware of a compromise, vulnerability or misuse affecting the Services.

8. Pennytel's enforcement rights

Where Pennytel reasonably believes that this policy has been, or may be, breached, we may investigate and take action proportionate to the nature and seriousness of the issue.

This may include:

- contacting you and asking you to stop or remedy the conduct;
- requiring reasonable information or written assurances;
- filtering, blocking, rate-limiting or restricting affected traffic or activity;
- temporarily suspending an affected Service; or
- terminating a Service where permitted under your agreement and applicable law.

Where reasonably practicable, Pennytel will notify you before taking enforcement action.

Pennytel may act immediately and without prior notice where this is reasonably necessary to:

- comply with applicable law, a court order, a regulator's direction or another lawful requirement;
- protect Pennytel's networks, systems, customers, suppliers or the public;
- prevent or respond to fraud, security threats, malware, denial-of-service activity or similar harmful conduct;
- avoid material harm or disruption; or
- prevent ongoing or serious misuse of the Services.

9. Monitoring, investigation and traffic management

Pennytel is not required to monitor all customer use of the Services. However, to the extent permitted by law and in accordance with our Privacy Policy, Pennytel may monitor, investigate, analyse, filter, block or restrict activity where reasonably necessary to:

- operate, maintain or protect the Services;
- investigate suspected breaches of this policy;
- respond to security incidents, fraud or network abuse;
- comply with legal or regulatory obligations; or
- enforce this policy and the applicable service agreement.

10. Site blocking and legally required restrictions

Pennytel may block, restrict or take other action in relation to access to websites, online locations, content, services, domains or traffic where required or authorised by applicable law, court order, regulator direction or other lawful process.

11. How to contact Pennytel

You can contact Pennytel in the following ways:

- **Phone:** 1300 232 888 Monday to Friday, 9:00am to 5:00pm AET
- **Email:** support@pennytel.com.au
- **Website chatbot:** Penny is available on the Pennytel website
- **Customer Portal:** Existing customers may also contact us directly through the Pennytel Customer Portal.

12. Complaints

If you have a complaint about this policy or how Pennytel has applied it, please contact us:

- **Email:** complaints@pennytel.com.au
- **Phone:** 1300 232 888

Pennytel will handle complaints in accordance with its **Complaints Handling Process** and applicable telecommunications complaints-handling requirements.

If you are not satisfied with how we have handled your complaint, you may contact the **Telecommunications Industry Ombudsman**, which is a free and independent dispute-resolution service for residential and small business customers:

- **Phone:** 1800 062 058
- **Online:** wwtio.com.au
- **Post:** GPO Box 276, Melbourne VIC 3001

13. Australian Consumer Law

Our services come with guarantees under the **Australian Consumer Law** that cannot be excluded. Nothing in this policy excludes, restricts or modifies your rights under the Australian Consumer Law.