

● ALL PEAR SERVICES

Acceptable Use Policy

What you may use a Pear service for, what you may not, how the spam rules work for email, SMS and MMS, and what happens if something goes wrong.

● SCOPE

01 · Who this policy applies to

This policy applies to every service supplied by Pear Australia Pty Ltd (ABN 94 624 986 554) — fixed telephone, mobile, internet, internet telephony and any other telecommunications service we provide (Services). In this policy, “we”, “us” and “our” mean Pear, and “you” and “your” mean the customer. It applies to anyone who uses a Service on your account — staff, family or anybody else you let use it.

By acquiring or using a Service you agree to comply with this policy. Capitalised terms not defined here have the meaning given in your Standard Form of Agreement, available on our website.

This policy governs the purposes a Service may be used for. Our Fair Use Policy governs how much you use a Service sold on an unlimited basis. Both apply, alongside your Agreement, and where a situation touches on both we may act under either or both.

You are responsible for how your Services are used, including by anyone you let use them. Anything that endangers a person, or risks compromising the security or operation of our network, systems or equipment — or those of our suppliers — may result in a Service being restricted, suspended or cancelled. Some Services also rely on upstream suppliers whose rules apply to you.

● UNLAWFUL

02 · Unlawful use

You must not use, attempt to use, or allow a Service to be used to:

- Breach any law, code or standard, incite violence or hatred, or do anything that could give rise to civil or criminal proceedings.
- Transmit or publish material that is defamatory, offensive, abusive, indecent, menacing, unwanted, unlawful, or that invades another person’s privacy.
- Send communications to anyone who has told you they do not want them, or send unsolicited advertising or bulk messages except in accordance with the Spam Act 2003 (Cth) — see section 04.

- Gain, or attempt to gain, unauthorised access to personal or commercially sensitive information, or to somebody else's account or password.
- Give false, misleading or deceptive information about yourself or your business in connection with a Service.
- Infringe anybody's intellectual property or other rights.

● MALICIOUS

03 · Malicious use

You must not use, attempt to use, or allow a Service to be used to:

- Compromise the security or integrity of any network or system, or probe, scan or test the vulnerability of any data, system or network.
- Access, store, send or distribute viruses, spyware or other harmful material.
- Interfere with, restrict or disrupt a Service, or another person's use of one.
- Overload, tamper with, hinder or make unauthorised modifications to any network or system, including our infrastructure.
- Access, monitor or use data or traffic on any system or network without authority.
- Disguise the origin of any use or communication, carry traffic for the purposes of arbitrage, or contact emergency service organisations where no emergency exists.
- Authorise, aid, abet, encourage or incite anybody else to do, or attempt, any of the above.

● SPAM

04 · Spam, marketing and unsolicited messages

The Spam Act 2003 (Cth) governs commercial electronic messages with an Australian link. It covers email, SMS, MMS and instant messaging — not just email. If you send marketing using a Pear Service, ten messages or ten thousand, you must comply with it. This section replaces our former Spam Acceptable Use Policy.

Three rules sit at the heart of the Spam Act. Every message must meet all three:

- Consent — express, or reasonably inferred from an existing relationship. You must be able to show where it came from, so keep a record.
- Accurate sender identification — every message must clearly identify you and carry contact details that work, including your business name and, where relevant, your ABN. You must not disguise the origin of a message or send from a spoofed address, sender ID or number.

- A functional unsubscribe — easy to use, costing no more than an ordinary message, live for at least 30 days, and honoured within 5 working days. For SMS and MMS, reply-STOP or the equivalent must work on the number the message came from.

You must also not send spam, allow it to be sent, or help anybody else send it, or use a Service to:

- Use, supply or acquire address-harvesting software, or use a list produced by it.
- Run an open mail relay or proxy that lets third parties send messages through your equipment.
- Otherwise breach the Spam Act 2003 (Cth) or the Do Not Call Register Act 2006 (Cth).

You must secure any device or network in your control — spam and virus filtering, antivirus software, a firewall, and patches applied when released. A compromised service is still your service: our right to act applies whether a breach is deliberate, the result of misconfiguration, or caused by malware. We may scan IP ranges allocated to you to detect open or misconfigured mail and proxy servers; where we find one we will tell you and give you a reasonable chance to fix it.

If you use Aria to message patients or clients

Our AI services can send SMS and email on your behalf — appointment reminders, recalls, results notifications. Using our tools does not transfer your obligations to us. You remain the sender: you need consent, your messages must identify you accurately, and an unsubscribe or opt-out must work and be honoured within five working days. If you handle health information you also remain responsible under the Privacy Act and the Australian Privacy Principles for what you send and to whom. We will help you set it up properly — ask us before you launch a campaign.

● UNREASONABLE

05 · Unreasonable use

Plans are priced for the purpose they are sold for. Use is unreasonable if a Service, plan inclusion, promotion or offer is used outside the ordinary purpose of that plan — a residential plan sold for household use being used commercially, for example.

Use outside the ordinary purpose of a plan includes:

- Running a telemarketing business or call centre on a plan not sold for that purpose.
- Re-supplying or reselling the Service.
- Wholesaling any Service — transit, refil or the aggregation of domestic or international traffic.
- Abnormal or excessive use of back-to-base services.

- SIM boxing, or using a Service or one of our SIM cards with a device or method that switches, routes or re-routes traffic to or from our network or a supplier's network.
- Use that affects other customers' access to the network or their enjoyment of the Services.
- Setting up switching devices that circumvent subscription or pricing arrangements.

We may treat other conduct as unreasonable, but only where it is of the same kind as the examples above — commercial rather than ordinary, machine-generated rather than human, resold beyond your business or household, or degrading the service others receive. Heavy or unusual use is not, by itself, unreasonable.

This section is about what you use a Service for, not how much. If you are on an unlimited plan and the question is volume, our Fair Use Policy applies and its two-step process is what you can expect. Where both are in play — dialler traffic on an unlimited plan — we may act under either or both.

● EQUIPMENT

06 · Your equipment and your content

You are responsible for providing, configuring and maintaining the equipment and software you need to access the Services, and for the security of your own data — in particular for protecting equipment from unauthorised third parties using your hardware or software. That does not apply to anything we have agreed to manage for you. You are also responsible for content you store, send or distribute over our network, even where somebody else has gained access to your Service.

We are not responsible for the content available through the Services, and use of them is at your own risk. The internet is not secure, it carries harmful material, and it is not controlled by us. Nothing here limits your rights under the Australian Consumer Law.

● LAW

07 · Law enforcement, regulators and monitoring

We are required by law to assist law enforcement agencies, and may have to comply with a lawful request at any time without notice to you. Where we do, we act in accordance with our legal obligations, including under the Telecommunications (Interception and Access) Act 1979 (Cth). Our Privacy Policy, available on our website, explains how we handle customer information. We must also refer a customer to the Australian Federal Police where we have reason to believe a Service has been used to access child sexual abuse material. We may monitor traffic and published content to check compliance with this policy, only as far as the law allows and for no other purpose.

BREACH

08 · What happens if you breach this policy

1**First — we contact you.**

If we believe on reasonable grounds that you have breached this policy, we will contact you, explain what we have seen and ask you to change how the Service is used. You get a reasonable time to fix it — what is reasonable depends on how serious the problem is and how much harm it causes.

2**If it is not fixed — we may restrict or suspend.**

We may restrict or suspend a Service until the problem is resolved. If the grounds are not corrected to our reasonable satisfaction within 7 days, we may cancel it — and if we do, you may apply for a pro rata refund of prepaid charges. We may charge a reasonable fee for costs we incur.

3**Other steps we may take.**

We may inform regulators or law enforcement of suspected illegal conduct, remove or edit your content stored on our systems, override an attempt to breach this policy such as by specifying a traffic routing pattern, recover the reasonable costs of identifying an offender, or decline to supply you in future — and we may do any of these if a regulator or law enforcement body directs us to.

Serious cases — immediate action

Where use is plainly illegal, threatens the network, involves fraud, or puts a person at risk, we may suspend or cancel a Service immediately and without the notice above, in accordance with your Agreement. We reserve that for those cases. Even then we will contact you first where it is safe and lawful to do so — and where it is not, as soon as it is — and tell you what we need to restore the Service. This mirrors our Fair Use Policy: two steps where use has drifted, immediate action only for deliberate abuse.

CHANGES

09 · Changes, questions and reporting a breach

We may vary this policy on the notice set out in your Agreement. Continuing to use the Services after a variation takes effect means you accept it. The current version is always available on our website.

To report a suspected breach — including a Pear service being used to send you spam — email support@peartelco.com.au with as much detail as you can. If you disagree with something we have done under

this policy, raise it under our Complaint Handling Policy, or take it to the Telecommunications Industry Ombudsman on 1800 062 058 or tio.com.au.

● TALK TO US

Not sure whether something is allowed? Ask.

Call 1300 007 327 or email hello@peartelco.com.au. Report a suspected breach to support@peartelco.com.au. We would much rather have the conversation before it becomes a problem.