

Acceptable Use and Fair Use Policy

The rules for using FlixLink services fairly and safely.

Effective date: 1 November 2026 · Version 1.0

FlixLink · Flixlink Broadband Pty Ltd, ABN 44 669 575 679 · (02) 9071 2900 · info@flixlink.com.au · flixlink.com.au

This policy sets out the rules for using FlixLink's internet, phone, mobile and managed services, so they stay safe, legal and reliable for everyone. It explains what you can't use our services for (such as illegal activity, scams, spam, hacking and copyright infringement), what "unlimited" means on our plans, how to report abuse or harmful content, and the fair, step-by-step approach we take if the rules are broken.

1. About this policy

This policy is part of your agreement with Flixlink Broadband Pty Ltd (ABN 44 669 575 679), trading as FlixLink Telecommunications ('FlixLink', 'we', 'us', 'our'), together with our Customer Terms and the Critical Information Summary for your plan.

It applies to all our services, including:

- internet services, such as nbn®, Opticomm fibre, business and enterprise internet, Home Wireless Broadband and 5G Home Broadband;
- voice services, such as nbn Voice, SIP trunking, Cloud Office UC and 13, 1300 and 1800 numbers;
- mobile and mobile broadband services;
- managed services, such as managed internet, managed Wi-Fi and security, and IP-VPN and MPLS.

"You" means the account holder. You're responsible for making sure that anyone you let use your service, such as people in your household or your staff, follows this policy. If someone uses your service without your permission, for example after your Wi-Fi or phone system is hacked, tell us as soon as you can and we'll take that into account.

Nothing in this policy limits your rights under the Australian Consumer Law or any other law.

2. Use our services lawfully and respectfully

You must not use a FlixLink service, or let anyone else use it, to:

- break the law, or help someone else break it;
- commit fraud, identity theft or scams;
- threaten, harass, stalk, menace or abuse anyone (using a phone or internet service to do this can be a crime);
- access, store, share or send child sexual abuse material, or material that promotes, incites or instructs in terrorism or violent crime;
- share, or threaten to share, intimate images of someone without their consent;
- intercept or record other people's communications unlawfully;
- collect or misuse other people's personal information unlawfully;

- infringe other people's copyright or other rights (section 3).

If your phone system records calls, you're responsible for telling callers and following the laws about recording calls.

We don't check the content you send or receive, and you're responsible for your own content. But if we become aware of child sexual abuse material or abhorrent violent material involving our services, we'll report it to the Australian Federal Police. We also follow lawful directions from the eSafety Commissioner and other authorities, such as directions to block access to certain material.

3. Copyright and other people's rights

- Don't use our services to copy, download, share or stream material in a way that infringes copyright, such as pirated films, TV shows, music, games or software. Don't infringe trade marks or other intellectual property.
- If a copyright owner tells us your service has been used to infringe copyright, we may contact you about it. We won't give your details to the copyright owner unless you agree, or the law or a court requires it.
- If your service keeps being used to infringe copyright after we've warned you, we may suspend or cancel it in appropriate circumstances, following the steps in section 10. Having this kind of policy for repeat infringers is one of the conditions the Copyright Act 1968 sets for providers like us.
- We must follow court orders that require us to block access to certain websites.

4. Spam, marketing messages and telemarketing

If you use our services to send marketing emails or texts, or to make telemarketing calls, you must follow the law, including:

- **the Spam Act 2003:** only send commercial emails and texts to people who have consented, identify yourself accurately, and include a free, working way to unsubscribe that you act on within 5 working days. Don't use address-harvesting software, or lists made with it;
- **the Do Not Call Register Act 2006:** don't make telemarketing calls to numbers on the Do Not Call Register without consent;
- **the Telecommunications (Telemarketing and Research Calls) Industry Standard 2017:** for example, only call at permitted times, and show a caller ID number that can be called back.

You must not use our services to send spam (bulk or unsolicited messages) by email, text or any other messaging. Our mobile and residential plans aren't designed for bulk messaging (section 8).

If spam sent from your service causes other networks to block our network or IP addresses, we may restrict sending from your service (for example, outgoing email) until the problem is fixed, as explained in section 10.

5. Scam calls and texts, caller ID and sender IDs

Scammers often pretend to be trusted people and businesses. To protect everyone:

- **No scams.** Never use our services to make scam calls, send scam texts or phishing messages, or pretend to be someone you're not.
- **Caller ID.** Your calls must only show a number that is valid and that you have the right to use. Don't hide or change your caller ID to mislead people (this is called spoofing). If you set your calls to show a different number from the one you're calling from, it must be a number you have the right to use. It can't be a freephone (1800) or local-rate (13 or 1300) number, or an invalid or unallocated number. See the ACMA's guide to caller ID scams.

- **Sender IDs.** If you send texts that show a business or brand name instead of a number, you must have a legitimate right to use that name, and it can't look like a phone number. Before we let you use it, you must give us evidence that you have a valid reason to use it, as clause 5.2.2 of the industry code C661:2022 Reducing Scam Calls and Scam SMS requires. You must also register it on the ACMA's SMS Sender ID Register. Since 1 July 2026, texts from unregistered sender IDs are shown as "Unverified".

What we must do. Under the C661:2022 code, we and other phone companies must identify, trace and block scam calls and scam texts, and share information about them with other providers and the ACMA. You can read more on the ACMA's Action on scams page. We may block calls or texts straight away if we reasonably believe they're scams. If a service is used for scams, we may restrict, suspend or cancel it (section 10).

If you get a scam call or text, report it to Scamwatch. If it came from a FlixLink number, tell us too (section 9).

6. Security and protecting the network

You must not use our services to:

- access, or try to access, any computer, network, account or data without permission, including probing or scanning other people's systems for weaknesses;
- carry out denial-of-service attacks, or deliberately overload a network or service;
- create or spread viruses, malware or ransomware, or control infected computers (botnets);
- host phishing websites or other scam content;
- run an open mail relay, open proxy, open DNS resolver or similar service that other people can misuse;
- get around our security, identity checks, usage metering or billing;
- interfere with our network, our suppliers' networks or other customers' services, for example by tampering with network equipment or connecting equipment that causes interference.

Look after your own security:

- Change the default passwords on your modem and devices, use strong passwords, and keep software up to date.
- Keep your account passwords, PINs and one-time codes private. Only read out a code to us if you contacted us first or asked to move your number. See Account Security and Scam Protection Policy.
- If you have a business phone system, keep its passwords and SIP account details secure. Criminals who break into phone systems can make large numbers of expensive calls.

If we find out that a device on your service is infected or being misused, for example from another network or a security organisation, we'll tell you so you can fix it. If it's needed to protect other people or the network, we may restrict the affected part of your service until it's fixed (section 10).

We and our suppliers may monitor network activity and traffic patterns, but not the content of your communications, to keep the network secure, detect fraud and scams, and meet our legal obligations.

7. No resale without our agreement

- Residential plans are for personal and household use at your premises. Business plans are for the normal use of your business.

- You must not resell, resupply or charge others for our services, or share a service with other premises, unless we've agreed in writing. For example, you can't sell access to your connection to neighbours or other businesses.
- Business customers can let staff and visitors use the service at their premises (for example, guest Wi-Fi) as part of running the business, but can't sell it as a phone or internet service.
- If you'd like to resell our services, ask us about a separate written agreement.

8. Fair use of "unlimited" plans

"Unlimited" means you can use the included feature as much as you need for its normal purpose, with no cap and no extra charge. Fair use makes sure plans are used for what they're designed for, so they stay good value for everyone.

Unlimited data

Plans with unlimited data, such as our nbn home broadband, Home Wireless Broadband and 5G Home Broadband plans, have no data cap. Use the data as much as you like for normal residential or business use, such as streaming, gaming, working from home and uploading. Fair use means you don't:

- resell the service or share it beyond your premises (section 7);
- use it as a wholesale link, or to supply other premises or customers;
- use it in a way that breaks sections 2 to 6.

Unlimited calls and texts

Unlimited standard national calls and texts on our mobile plans, and unlimited calls on any voice plan that includes them, are for normal person-to-person use by you, your household or your business. They're not for:

- call centres or telemarketing;
- auto-diallers, robocalls or recorded-message calls;
- bulk or automated texts;
- reselling or wholesaling calls or texts, or carrying other people's traffic;
- SIM boxes, GSM gateways or similar devices that pass calls or texts from other networks or internet calling services into the mobile network.

If your business needs this kind of use, ask us about a plan designed for it.

Mobile data, extra charges and alerts

Our mobile plans include a monthly data allowance. Extra data and roaming packs are charged as set out in your Critical Information Summary. Ask us for international call and roaming rates before you use them. We send you free usage alerts when you've used 50%, 85% and 100% of your included data, and roaming alerts when you use your mobile overseas.

How we apply fair use

- We look at the pattern of use over time, not one busy day or month. Heavy normal use isn't a breach.
- If your use looks like one of the uses this section rules out, we'll contact you first, explain why, and give you at least 14 days to tell us your side, change how you use the service, or move to a plan that suits your use.

- We'll only take further steps under section 10 if the use continues, unless section 10 allows us to act straight away (for example, to stop fraud).

9. Reporting abuse and harmful content

Report abuse to us

Tell us if you think a FlixLink service is being used for spam, scams, hacking, copyright infringement, harassment or any other breach of this policy.

- Email info@flixlink.com.au with 'Abuse report' in the subject, or call (02) 9071 2900.
- Include as much detail as you can: what happened, the date and time (with the time zone), and the phone number, IP address, email headers or web address involved.

We look into every report. Because of privacy law, we usually can't tell you what action we've taken about another customer.

Report harmful online content to eSafety

The eSafety Commissioner handles complaints about:

- illegal and harmful online content, such as child sexual abuse material, and material that promotes, incites or instructs in terrorism or violent crime;
- cyberbullying of children;
- online abuse of adults;
- image-based abuse (sharing, or threatening to share, intimate images without consent).

Report it at esafety.gov.au/report. If you're in immediate danger, call Triple Zero (000).

Other places to get help

- **Scams:** report to Scamwatch. If you've lost money, contact your bank first.
- **Identity theft:** IDCARE gives free support on 1800 595 160, or at idcare.org.
- **Spam and telemarketing:** see the ACMA's page on how to reduce or report spam, and the Do Not Call Register.

10. What we do if this policy is breached

We act fairly and in proportion to the problem. We consider how serious it is, whether it was deliberate or is continuing, the risk of harm to other people or the network, and your circumstances.

Our usual steps

1. **We tell you.** We contact you in writing, explain the problem, and give you at least 14 days to stop or fix it.
2. **We restrict the service.** If the problem continues, we may restrict the part of the service involved, for example by blocking outgoing texts, outgoing email or international calls.
3. **We suspend the service.** If restricting it isn't enough, or the problem still continues, we may suspend the service.
4. **We cancel the service.** As a last resort, for a serious or repeated breach, we may cancel the service. We'll give you written notice first.

We follow these steps in order, unless the next part of this section allows us to act straight away.

When we may act straight away

We'll only restrict or suspend a service without telling you first if that's reasonably necessary:

- to prevent harm to a person;
- to stop fraud, identity theft, a scam or other illegal activity;
- to protect our network, our suppliers' networks or other customers; or
- to follow the law, a court order, or a direction from a regulator, emergency service or government agency.

We'll limit what we do to what's needed, for only as long as it's needed. We'll tell you as soon as practicable what we've done and why, and what you need to do to restore the service, unless the law stops us from telling you.

Your rights

- You can tell us your side at any time, and we'll consider it.
- If you've told us you're affected by domestic, family or sexual violence, the protections in our Domestic, Family and Sexual Violence Support Policy policy also apply.
- This policy isn't about unpaid bills. Our Customer Terms and Financial Hardship Policy policy cover those.
- If we restrict, suspend or cancel a service by mistake, we'll restore it promptly and won't charge a reconnection fee.
- If you disagree with what we've done, you can make a complaint. If you are not satisfied with how we have handled your complaint, you have a right to take it to the Telecommunications Industry Ombudsman, which is a free and independent service. Call 1800 062 058 or visit tio.com.au.

Charges

- Our Customer Terms explain what happens to your charges if a service is restricted, suspended or cancelled.
- If we cancel a fixed-term plan because of your serious or repeated breach, the early termination charge in your Critical Information Summary may apply. It's the same charge that applies if you cancel early yourself. It doesn't apply if we cancel for any other reason. Any remaining repayments for a modem you keep still apply.

Telling the authorities

If we reasonably believe a service is being used for a crime, we may report it to the police or other authorities, as the law allows. Our Privacy Policy explains when we can share information.

11. Changes to this policy

We may change this policy, for example to reflect changes in the law, our services or our network, or new kinds of misuse.

- If a change is to your detriment, we'll give you at least 30 days' notice by email or SMS. You can then cancel the affected service without paying an early termination charge. Any remaining repayments for a modem you keep still apply.
- For other changes, such as making the policy clearer, we'll publish the new version on our website with its effective date.

- If the law or a regulator requires a change sooner, we'll tell you as soon as practicable. If that change is to your detriment, you can still cancel without an early termination charge.

The current version is always on our website.

12. Contact us

- Phone: (02) 9071 2900
- Email: info@flixlink.com.au
- Website: flixlink.com.au
- Flixlink Broadband Pty Ltd, ABN 44 669 575 679, trading as FlixLink Telecommunications

nbn® is a trade mark of NBN Co Limited.