

1. Purpose

The Fibrenet Group is committed to providing reliable, secure and high-quality telecommunications services to all customers and users.

This Fair Use Policy explains:

- (a) your responsibilities when using our services;
- (b) what we consider to be unreasonable, unfair, excessive, unlawful or unacceptable use;
- (c) how we may monitor and manage use of our services to protect our network, systems, customers and users; and
- (d) the actions we may take where use of a service breaches this Policy.

This Policy is intended to ensure that no customer, end user or other person is unfairly disadvantaged by the conduct, usage patterns or security practices of another user.

2. Application

2.1 Who this Policy applies to

This Policy applies to all customers, end users and other persons who access or use services supplied by any company within the Fibrenet Group, including:

- a) Fibrenet Wholesale Pty Ltd;
- b) Fibrenet Broadband Pty Ltd;
- c) Interphone Pty Ltd;
- d) Fibrenet Australia Pty Ltd; and
- e) (e) any related body corporate, trading entity or business operated within the Fibrenet group of companies.

In this Policy, these entities are referred to as "Fibrenet", "we", "us" or "our".

2.2 Services covered by this Policy

This Policy applies to all telecommunications, internet, voice, data, network, managed, wholesale, retail and related services supplied by us.

It also applies to any equipment, infrastructure, platform, portal, website, application, network, system or facility used by us to supply those services.

2.3 Relationship with other terms

This Policy forms part of your agreement with us, including any service agreement, customer terms, wholesale agreement, application form, critical information summary, service order, acceptable use policy, or other terms applying to your service.

Where you are a wholesale customer, you must ensure that your customers and end users comply with this Policy.

2.4 Updates to this Policy

We may update this Policy from time to time. The current version will be made available on our website or otherwise provided on request.

3. Definitions

In this Policy:

"Customer" means the person or entity that has entered into an agreement with us for the supply of a service.

"End user" means any person who accesses or uses a service, whether directly or indirectly.

"Fibrenet Network" means any network, system, platform, equipment, facility, infrastructure or service operated, managed, supplied, resold or used by the Fibrenet Group.

"Service" means any telecommunications, internet, voice, data, wholesale, retail, managed or related service supplied by us.

"You" and **"your"** means the customer and, where applicable, any end user or person using the service.

4. Responsible Use

4.1 General responsibility

You must use the service responsibly, lawfully and in a way that does not:

- a) adversely affect the Fibrenet Network;
- b) adversely affect any other customer, end user or third party;
- c) compromise the security, integrity or performance of any network, service, system or equipment;
- d) expose us, another customer, an end user or any third party to liability, loss, harm or risk; or
- e) breach any applicable law, regulation, code, standard or industry requirement.

4.2 Security of your equipment and account

You are responsible for maintaining the security of your account, devices, systems and internal networks.

You must take reasonable steps to prevent your service from being used in breach of this Policy, including by:

- a) keeping usernames, passwords, access credentials and authentication methods secure;
- b) maintaining appropriate antivirus, endpoint protection, firewall and security controls where relevant;
- c) keeping operating systems, applications, firmware and connected devices reasonably up to date;
- d) ensuring that email servers, proxy servers, routers, wireless networks and other systems are not misconfigured or openly accessible in a way that may cause harm; and
- e) taking prompt action if you become aware of any compromise, misuse or suspected misuse of your service.

4.3 Residential services

If your service is supplied on a residential plan, you must use it in a manner that is consistent with ordinary personal, domestic or household use.

You must not use a residential service as a substitute for a commercial, carrier, wholesale, server hosting, public access, resale or high-volume business service unless we have agreed to that use in writing.

4.4 Business services

If your service is supplied on a business or commercial plan, you must use it in a manner that is consistent with the nature of that plan and the ordinary operational requirements of your business.

You must not use a business service for carrier-grade, wholesale, mass automation, public access, high-volume hosting, resale or other use outside the intended scope of the plan unless we have agreed to that use in writing.

4.5 Wholesale services

If you receive services from us as a wholesale customer, you must:

- a) ensure your personnel, contractors, customers and end users do not use the service in breach of this Policy;
- b) include appropriate terms in your own customer agreements that prohibit unreasonable, unfair, excessive, unlawful or unacceptable use;
- c) ensure you have the ability to suspend, restrict, disconnect or otherwise manage an end user service where required to address a breach of this Policy;
- d) promptly assist us to investigate, mitigate or stop any misuse of the service; and
- e) comply with any lawful or reasonable direction we give you in relation to network security, service integrity, misuse, spam, abuse, unlawful content, fraud, excessive use or other conduct covered by this Policy.

5. Unreasonable Use

5.1 What we consider unreasonable use

We may consider use of a service to be unreasonable if it is materially inconsistent with the nature, purpose, plan type, design or intended use of the service.

Examples of unreasonable use include:

- a) using a service for fraudulent, deceptive or misleading purposes;
- b) using a service for resale, redistribution, public access, wholesale supply or shared access unless we have agreed to that use in writing;
- c) using a residential service for commercial hosting, server operations, carrier services, call centre operations, mass communication, public Wi-Fi, managed network resale or other non-residential purposes;
- d) using a service in a way that avoids, bypasses or undermines normal charges, service limitations, plan inclusions, network management controls or billing arrangements;
- e) using a service for arbitrage, artificial traffic generation, traffic pumping, revenue share manipulation or similar activity;
- f) abnormal, excessive or automated use of voice, messaging, calling, signalling, alarm, back-to-base, machine-to-machine or similar services;
- g) using a service in a way that places an excessive or abnormal load on the Fibrenet Network;
- h) using a service in a way that materially degrades or may materially degrade the quality, performance or reliability of services supplied to other customers or users; or
- i) using a service in any other way that we reasonably consider to be outside the intended use of the service.

6. Unfair or Excessive Use

6.1 What we consider unfair or excessive use

We may consider use of a service to be unfair or excessive if it:

- a) creates a risk to the integrity, performance, availability or security of the Fibrenet Network;
- b) materially affects, or is likely to materially affect, the experience of other customers or users;

- c) consumes network resources in a manner that is excessive when compared with ordinary use by customers on the same or similar plan;
- d) causes or contributes to congestion, instability, degradation or abnormal network load;
- e) uses a service in a sustained, automated or abnormal manner not reasonably contemplated by the plan; or
- f) creates a risk to the health or safety of any person.

6.2 Unlimited plans

Where a plan is described as "unlimited", this means that the plan does not have a standard monthly data quota for ordinary use.

It does not mean that use of the service is infinite, unrestricted, unconstrained or able to be used in any manner.

Unlimited plans remain subject to this Policy, network management practices, service limitations and the intended use of the relevant plan.

6.3 Management of excessive use

Where your use is excessive, abnormal or unfair, we may take reasonable steps to manage that use, including:

- a) contacting you and asking you to reduce or modify your usage;
- b) working with you to move the service to a more suitable plan or service type;
- c) applying traffic management measures where reasonably necessary to protect the network or other users;
- d) limiting, shaping or prioritising certain traffic where reasonably necessary to manage congestion, security, abuse or network integrity;
- e) restricting or suspending the affected service; or
- f) terminating the affected service where the issue is not resolved or where immediate action is reasonably required.

7. Unacceptable and Prohibited Use

7.1 Prohibited conduct

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

- a) engage in unlawful, fraudulent, misleading, deceptive or malicious conduct;
- b) send, cause, facilitate or enable spam, unsolicited commercial electronic messages, phishing messages or other unwanted communications;
- c) distribute malware, ransomware, viruses, worms, trojans, spyware, botnet traffic or other harmful code;
- d) scan, probe, attack, interfere with, disrupt or attempt to gain unauthorised access to any network, system, device, account or data;
- e) compromise, attempt to compromise, or interfere with the security or operation of any network, system, device, account or service;
- f) monitor, intercept, collect or capture data or traffic without authorisation;
- g) obtain, use, disclose or interfere with another person's personal, private, confidential or sensitive information without authorisation;
- h) distribute, publish, transmit, host or make available content that is unlawful, defamatory,

- abusive, harassing, threatening, obscene, offensive, indecent or otherwise inappropriate;
- i) infringe or facilitate the infringement of intellectual property rights, including copyright;
- j) impersonate another person or entity, or misrepresent your identity, authority or affiliation;
- k) interfere with another person's use or enjoyment of any service, network, system or online platform;
- l) make hoax, nuisance, abusive, threatening or improper communications;
- m) contact emergency services where no emergency exists;
- n) breach any applicable law, regulation, industry code, standard, court order or lawful direction; or
- o) engage in any other conduct that we reasonably consider may expose us, another customer, an end user or any third party to liability, loss, harm or risk.

8. Content, Copyright and Lawful Directions

8.1 Customer responsibility for content

You are responsible for any content you access, publish, transmit, host, store, distribute or make available using the service.

We are not responsible for the content you access or make available using the service, except to the extent required by law.

8.2 Removal or restriction of content

We may block access to, remove, disable, restrict or refuse to host content where we reasonably consider that content:

- a) is unlawful;
- b) infringes intellectual property rights;
- c) is offensive, indecent, abusive, threatening, obscene or otherwise inappropriate;
- d) creates a risk to the Fibrenet Network, our customers or the public;
- e) breaches this Policy; or
- f) must be blocked, removed or restricted to comply with a lawful direction.

8.3 Law enforcement and regulatory requests

We may be required to cooperate with law enforcement agencies, regulators, emergency services, copyright owners or other authorised parties.

This may include disclosing account details, contact details, IP address information, traffic information, usage information or other identifying material where permitted or required by law.

Any disclosure of personal information will be handled in accordance with our Privacy Policy and applicable privacy laws.

9. Spam, Abuse and Network Protection

9.1 Spam and abuse management

To protect the Fibrenet Network and other users, we may take steps to reduce spam, abuse, malicious traffic or harmful activity.

These steps may include:

- a) filtering, rate-limiting, blocking or rejecting email, traffic, ports, protocols or destinations;
- b) restricting the ability to forward, relay or send email;

- c) requiring you to fix misconfigured mail servers, proxy servers, DNS servers, routers or other systems;
- d) suspending compromised accounts, devices or services;
- e) limiting access to a closed user group or controlled network environment where appropriate; or
- f) requiring reasonable security changes before restoring full service.

9.2 Compromised services

If we reasonably suspect that your service, equipment, account or network has been compromised or is being used to cause harm, we may take urgent action to protect the Fibrenet Network, other customers, end users or third parties.

This may include restricting, suspending or isolating the affected service without prior notice where immediate action is reasonably required.

10. Monitoring Compliance

10.1 Monitoring of the network

We are not required to actively monitor all use of the Fibrenet Network.

However, we may monitor, investigate, analyse or manage network usage, traffic patterns, service performance, security events, abuse reports, faults, complaints or other information where reasonably required to:

- a) operate, maintain, secure and protect the Fibrenet Network;
- b) identify or prevent misuse, fraud, spam, malware, security threats or unlawful activity;
- c) manage congestion, faults, performance or network integrity;
- d) comply with legal, regulatory, industry or contractual obligations;
- e) investigate complaints or suspected breaches of this Policy; or
- f) protect our customers, end users, personnel, systems, suppliers and the public.

10.2 Privacy

Any monitoring or handling of personal information will be carried out in accordance with our Privacy Policy and applicable privacy laws.

11. Notice and Action We May Take

11.1 Where we will usually give notice

Where your use of the service breaches this Policy, and the circumstances are not urgent, serious, unlawful, harmful or security-related, we will usually contact you and give you a reasonable opportunity to stop or remedy the breach.

This may include asking you to reduce usage, change usage patterns, fix a misconfiguration, secure a device, remove content, stop prohibited activity, or move to a more suitable service.

11.2 Restriction, suspension or disconnection

Where we propose to restrict, suspend or disconnect a residential or small business service due to a breach of this Policy, we will provide notice where required by applicable laws, codes, standards or industry requirements.

Where required, this will include giving you fair warning and a reasonable opportunity to avoid restriction, suspension or disconnection.

11.3 Urgent action without prior notice

We may restrict, suspend, disconnect, block, rate-limit, isolate or otherwise manage a service immediately and without prior notice if we reasonably believe that urgent action is required because:

- a) the service is being used unlawfully;
- b) the service is being used for fraud, abuse, spam, malware, hacking, phishing, security compromise or other harmful activity;
- c) the service creates an immediate or material risk to the Fibrenet Network;
- d) the service creates a risk to another customer, end user, third party or the public;
- e) we are required to do so by law, a regulator, law enforcement agency, emergency services organisation, court, network supplier or upstream provider;
- f) the service is materially interfering with the operation of the Fibrenet Network or another service; or
- g) the service is being used in a way that is plainly outside the intended use of the service.

11.4 Possible actions

Depending on the circumstances, we may:

- a) issue a warning or request that you stop or change the relevant use;
- b) require you to secure, reconfigure or disconnect equipment;
- c) require you to remove or disable content;
- d) block or filter traffic, ports, protocols, destinations, domains, URLs or services;
- e) apply rate limits, traffic shaping or other network management controls;
- f) move you to a more suitable service or plan, where available and agreed;
- g) restrict, suspend or disconnect the service;
- h) terminate the service in accordance with your agreement with us;
- i) report the matter to law enforcement, a regulator, a network supplier, an upstream provider or another authorised party; or
- j) take any other lawful and reasonable step required to protect the Fibrenet Network, our customers, end users or third parties.

12. Data, Files and Service Termination

Where a service is terminated, suspended or disconnected, we may delete, disable, remove or cease storing any files, data, configurations, content, mailboxes, hosting material or other information associated with the service, subject to your agreement with us and applicable law.

You are responsible for maintaining your own backups of any data, content or files that you upload, store, transmit or host using the service.

13. Your Liability

You are responsible for all use of your service, including use by any person who accesses the service with your permission or through your equipment, premises, account, credentials or network.

You may be liable for any loss, cost, expense, claim, damage or liability suffered by us or any third party as a result of your breach of this Policy, except to the extent caused by our negligence, wilful misconduct or breach of law.

14. Complaints and Disputes

If you disagree with any action we take under this Policy, you may contact us and raise a complaint.

We will handle complaints in accordance with our Complaints Handling Policy and applicable telecommunications consumer protection requirements.

You may also have external dispute resolution rights, including through the Telecommunications Industry Ombudsman where your service is eligible.

15. Contact Us

If you have any questions about this Policy, or if you believe your service has been restricted, suspended or otherwise affected in error, please contact us using the contact details available on our website.