ACCEPTABLE USE POLICY

Business 1300 Pty Ltd ACN 108 753 751

Last Updated: 17 February 2026

1. About This Policy

(a) This is Business1300's Acceptable Use Policy (Policy). In this Policy a reference to 'Business1300' or 'we' or 'us' or 'our' means Business 1300 Pty Ltd (ACN 108 753 751) and its related bodies corporate within the meaning of the Corporations Act 2001 (Cth).

(b) This Policy aims to ensure we can continue to provide high quality telecommunication services (including but not limited to telephone, internet, mobile phone, internet telephony and other telecommunications services) (**Services**) to all Customers in compliance with applicable laws, including the Telecommunications Act 1997 (Cth), the Telecommunications Consumer Protections Code (C628:2019), and other applicable industry codes.

(c) This Policy also looks to safeguard the security and integrity of the infrastructure and systems which we use to deliver Services in order to maintain them consistently for the common benefit of all users.

(d) This Policy is also intended to ensure that our Customers do not use our Services in an excessive, unreasonable or fraudulent manner where such use may impact the quality and reliability of the Services including our ability to provide the Services.

(e) The Policy applies to all our Services. It sets out Customers' responsibilities when using our Services and confirms the steps we may take to ensure and monitor compliance with this Policy.

(f) Capitalised terms not defined in this policy have the meaning given to them in the Customer Terms, a copy of which is available on our website (**Customer Terms**).

2. When Does This Policy Apply?

This Policy applies to all Customers and any users of our Services. By acquiring or using any of our Services, you acknowledge that you have read, understood, and agree to comply with the terms of this Policy. We may rely on this Policy where a Customer or other end users' use of a Service is:

(a) not in accordance with this Policy; and/or

(b) reasonably considered to be use outside the purposes of the relevant Plan.

3. General Responsibility for Behaviour

(a) Every end user is responsible for their use of our Services, network and the operation of any systems or applications accessed or used with our Services. All Customers agree they will not use, attempt to use or allow their Service to be used for any unlawful or malicious purpose.

(b) Any act that endangers any person or risks endangering or compromising the security or effective operation of our network, or any of our systems or equipment (or the network, systems or equipment of our suppliers), may result in immediate restriction, suspension or termination of access to a Service in accordance with the Contract and this Policy, and where required by law, we will report such conduct to relevant authorities.

(c) When using a Service, users must comply with rules imposed by our upstream suppliers or third parties from which you access content. Where a supplier or third-party provider notifies us that one of our Customers is in breach of this Policy or their terms, we may be required to take action to prevent the relevant Customer from continuing such breach, including suspension or termination of the Service.

(d) If a Customer fails to comply with the Customer Terms or this Policy, we may suspend or cancel a Customer's use of, or access to, some or all Services.

4. More Specific Examples of Conduct Which May Breach This Policy

Further to the general rights and responsibilities set out above and in the Customer Terms, all Customers agree they will not use, attempt to use or allow their Service to be used to:

(a) breach any law, code or standard;

(b) transmit, publish or communicate material which is defamatory, offensive, abusive, indecent, menacing, unwanted or violates the privacy of another party;

(c) distribute communication to a person or group who has indicated that they do not wish to receive the communication from the Customer;

(d) store, send or distribute any content which is restricted, prohibited or unlawful under any applicable law, or that is likely to offend a reasonable person;

(e) send or distribute unsolicited advertising or bulk messages in breach of the Spam Act 2003 (Cth) or the Do Not Call Register Act 2006 (Cth);

(f) do anything which incites violence or hatred against, any person or class of persons, or which could give rise to civil or criminal proceedings;

(g) gain unauthorised access to a person's private or personal information or a company's commercially sensitive information (or attempt to do either);

(h) use another person's name, username or password or attempt to gain access to the account of any person;

(i) provide false, misleading or deceptive information about yourself or your business to us or any other person in relation to your use of the Services or in order to gain access to a Service or a Service feature;

(j) infringe any person or company's intellectual property or other rights;

(k) compromise the security or integrity of any network or system;

(l) access, download, store, send or distribute viruses, spy software or other harmful material;

(m) interfere, restrict or disrupt Services or any other person or company's use or enjoyment of Services;

(n) use the Service to communicate with emergency service organisations where an emergency situation does not exist;

(o) disguise the origin of a use or communication;

(p) access, monitor or use any data or traffic on any systems or networks without authority;

(q) attempt to probe, scan or test the vulnerability of any data, system or network;

(r) use the Services for the purposes of arbitrage;

(s) overload any network or system including our infrastructure, network and/or systems;

(t) tamper with, hinder the operation of or make unauthorised modifications to any network or system;

(u) authorise, aid, abet, encourage or incite any other person to do or attempt to do any of the above acts.

5. Responsibility for Content

Customers acknowledge that:

(a) we are not responsible for the content of the Services;

(b) use of the Services is at the Customer's sole risk;

(c) subject to any rights under the Australian Consumer Law which cannot be excluded, we are not liable for any unsolicited or unwelcome information disseminated via the Services to the Customer or the consequences of the Customer receiving such information;

(d) the Internet:

i. is not necessarily a secure and confidential method of communication and the Customer transmits data at their own risk; and

ii. contains viruses, Trojan programs, spy software and other harmful material that may destroy or corrupt Customer's own system; and

iii. is not controlled by us and, subject to any rights under the Australian Consumer Law which cannot be excluded, we are not liable for any damage to, or loss of data caused by material accessed on the internet.

6. Responsibility for Maintenance and Security

(a) Customers are responsible for providing, configuring or maintaining any equipment or software they need to access the Service, as well as for the security and integrity of Customer's data (in particular for protecting equipment from unauthorised third parties using your hardware or software) except where we have agreed to provide and manage certain equipment or software.

(b) Customers are responsible for maintaining the security of Service account details, passwords and protection against unauthorised usage of the Service by a third-party. Subject to your rights under the Australian Consumer Law and our obligations under the Telecommunications Consumer Protections Code, you are responsible for charges incurred due to unauthorised usage of the Service.

7. Unreasonable Use

Without limiting the meaning of 'unreasonable', we may consider Customer use of a Service, Plan inclusion, promotion and/or offer to be unreasonable if accessed or utilised for purposes including but not limited to:

(a) running a telemarketing business or call centre;

(b) re-supplying or reselling the Service;

(c) wholesale of any Service (e.g. transit, refile or aggregate domestic or international traffic) on our network;

(d) abnormal or excessive use of back to base services;

(e) SIM boxing or using the Service (including any of our SIM card(s)) in connection with a device or method that switches, routes or reroutes traffic (e.g. calls, SMS, data, etc.) to or from the our network or the network of any supplier;

(f) usage that affects other Customers' access to the network or enjoyment of the Services;

(g) setting up switch devices which overcome subscription and/or pricing charges, potentially limiting the ability for other Customers to access the Service; or

(h) any other activity which would not be reasonably regarded as typical or ordinary use.

8. Excessive Use

Excessive use is a continuing and unreasonably disproportionate use of the Service when compared to the average usage of other Customers on comparable plans. We may consider Customer use of a Service, plan inclusion, promotion and/or offer to be excessive in the following examples:

(a) more than 5% of calls being in excess of 60 minutes duration;

(b) more than 2,000 minutes of talk time per month per Service;

(c) calls to a monitored alarm service exceeding six (6) times per day.

Where our systems detect usage approaching the thresholds set out in this section, we may (but are not obligated to) provide advance notice to the Customer via email or SMS. Such notice does not limit our rights under this Policy where usage subsequently exceeds the thresholds or where the Customer fails to modify usage following such notice.

9. Lawful Use

(a) Customers must ensure that any use of our Services is lawful and it is their responsibility for determining the content and information they choose to access when using a Service, even if they were used without the Customer's consent, by another person who gains access to them.

(b) Customers are responsible for any content stored, sent, accessed or distributed on or via our Network and systems including content posted on web pages, email, social media, chat or discussion forums, bulletin boards, instant messaging and SMS.

(c) Customers must not use Services to send or distribute content which is prohibited or otherwise unlawful under any applicable Australian law or in breach of an applicable Agreement. If Customers provide content using the Services it is the Customer's responsibility to comply with the Broadcasting Services Act 1992 (Cth), the Online Safety Act 2021 (Cth), any applicable Industry Codes and any other applicable law. We are required by law to refer a Customer to the Australian Federal Police if we have reason to believe a Service has been used to access, transmit, or possess child abuse material as defined under the Criminal Code Act 1995 (Cth).

10. Regulatory Authorities

At law, we are required to assist law enforcement agencies. We may be required to comply with law enforcement or other lawful requests at any time without notice to Customers but in doing so will act in accordance with our legal obligations, including under the Telecommunications (Interception and Access) Act 1979 (Cth) and the Telecommunications Act 1997 (Cth).

11. Breach of Policy – Our Rights

(a) If we believe on reasonable grounds that a Customer has breached this Policy, we may contact you and ask you to modify your use of the Service.

(b) Progressive Enforcement: where reasonably practicable, we will apply proportionate enforcement measures appropriate to the nature and severity of the breach. However, we may take immediate action without prior notice or warning where:

i. the breach poses an imminent risk to network security, integrity or availability;
ii. the breach involves illegal activity;
iii. the breach causes or is likely to cause material harm to other Customers' use of Services;
iv. we are directed to do so by a law enforcement or regulatory body; or
v. the Customer has previously been notified of similar breaches.

(c) We also specifically reserve the right to take one or more of the following steps:

i. suspend access to the Service indefinitely or for a specific period;
ii. terminate access to the Service and refuse to provide the Service to the Customer or their associates in the future;
iii. inform appropriate government and regulatory authorities of suspected illegal or infringing conduct;
iv. delete or edit any of the Customer's data (including webpage content) stored on systems;

v. override any attempt by the Customer to breach this Policy, such as specify a particular traffic routing pattern; and

vi. take any other action we deem appropriate, including taking action against offenders to recover our reasonable costs and expenses, which may include:

a. costs of investigating the breach;

b. technical costs of remediation or restoring service to other affected Customers;

c. costs imposed on us by upstream suppliers or third parties as a result of the breach;

d. legal costs of enforcement; and

e. any fines or penalties imposed on us by regulatory authorities as a result of the Customer's breach.

(d) We may also take any of the above steps if directed to do so by a regulatory or other law enforcement body.

(e) Our right to suspend access to Services without notice under clause 11(b) overrides any requirement we may have to give notice under the Customer Terms. For all other breaches, we will comply with applicable notice requirements in the Customer Terms unless providing notice would compromise our ability to address the breach or would violate our obligations to law enforcement or regulatory authorities.

12. Investigation of Suspected Breaches

(a) Where we identify potential breaches of this Policy through automated monitoring, customer complaints, or notices from upstream providers or third parties, we will conduct a reasonable investigation before taking enforcement action, except where immediate action is required under clause 11(b).

(b) We will consider reasonable grounds to exist where:

i. our automated systems detect usage patterns consistent with prohibited or excessive use as defined in this Policy;

ii. we receive multiple independent complaints regarding a Customer's use of Services;

iii. an upstream supplier or third-party provider notifies us of a breach;

iv. law enforcement or regulatory authorities advise us of suspected illegal activity; or

v. our network monitoring reveals activity consistent with security threats, unauthorised access attempts, or system vulnerabilities being exploited.

(c) Where we contact a Customer regarding suspected excessive or unreasonable use, we will provide the Customer with reasonable particulars of the suspected breach and a reasonable opportunity (typically 5 business days unless otherwise specified) to respond before taking further enforcement action, except where immediate action is required under clause 11(b).

13. Reinstatement After Suspension

(a) Where a Service has been suspended for excessive or unreasonable use (but not for illegal activity or security threats), a Customer may request reinstatement by:

i. providing a written undertaking to modify usage patterns to comply with this Policy;

ii. paying any outstanding charges or fees associated with the breach; and

iii. where applicable, agreeing to migrate to a plan more appropriate for the Customer's usage requirements.

(b) We will consider reinstatement requests within 2 business days and may impose conditions on reinstatement, including monitoring periods, usage limits, or plan changes.

(c) Where a Service has been suspended for illegal activity, security breaches, or repeated violations after prior warnings, we reserve the right to refuse reinstatement and proceed to termination.

14. Policy Changes

We may vary this Policy from time to time but will do so in line with the relevant notice provisions in your Agreement. Continued use of Services after receiving notice once the variation takes effect will constitute acceptance of the variation.