# ACCEPTABLE USE POLICY

commander

## 1. ABOUT THIS POLICY

This document is the Commander Acceptable Use Policy **(Policy)** and this Policy aims to ensure Commander can continue to provide high quality telecommunications 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 and industry codes.

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 and other suppliers of telecommunications.

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.

Capitalised terms not defined in this Policy have the meaning given to them in the Agreement available at https://www.commander.com.au/customer-terms **(Agreement)**.

## 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 are taken to have agreed 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

- not in accordance with this Policy; and/or
- reasonably considered to be use outside the purposes of the relevant Plan.

## 3. GENERAL RESPONSIBILITY FOR BEHAVIOUR

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, unsafe, abhorrent or malicious purpose.

Any act that endangers any person (including cyber bullying) 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 mean access to a Service will be restricted, suspended or terminated in accordance with the Agreement and this Policy.

When using a Service, we may require users to comply with rules imposed by our upstream suppliers or from a third party from which you access content. Where a supplier or third party provider considers one of our Customers is in breach of this Policy, they may require we prevent the relevant Customer continuing to breach this Policy.

If a Customer fails to comply with these obligations, we may suspend or cancel a Customer's use of or access to some or all Services.

### More specific examples of conduct which may breach this Policy

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

UNLAWFUL USE

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, including all sexual content, violent or not;

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 be offend a reasonable person;

e) send or distribute unsolicited advertising or bulk messages as defined in the Spam Act 2003 or otherwise breach our Spam policy;

f) do anything which promotes, incites, instructs in or depicts violent conduct 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; or

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

MALICIOUS USE

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, including any malware that could potentially be installed to send infected messages;

m) including excessive data use in breach of service policies, 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) including excessive data use in breach of service policies, overload any network or system including our infra structure, 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.

### Provider not responsible 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) 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) Services are provided without warranties of any kind, either express or implied, unless such warranties are legally incapable of exclusion; and
e) 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 we are not liable for any damage to, or loss of data caused by material accessed on the internet.

Customers are responsible for providing, configuring or maintaining any equipment or software they need to access the Services, 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.

## 4. UNREASONABLE USE

Commander considers Customer use of a Service, plan inclusion, promotion and/or offer to be unreasonable if accessed or utilised for any non-ordinary purpose or if the Plan is a residential plan for household or personal use only, but is instead used for commercial or other untypical household or personal purposes.

Unless the Services are provided by us for that purpose and the specific terms and conditions relating to the Service or Plan provide in writing for commercial or non-ordinary purposes. We may give or withhold consent, or give consent subject to any conditions, at our sole discretion.

Non-ordinary purpose includes:

a) running a telemarketing business or call centre;
b) re-supplying or reselling the Service or facilitating the provision of services to multiple premises, (such as an apartment building, shopping centre, business park, or residential/retirement village) and using that service to facilitate the provision to multiple premises within that multi-premises site;
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 our SIM card) in connection with a device or method that switches, routes or re-routes traffic (e.g. calls, SMS, data, etc.) to or from 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.

## 5. REGULATORY AUTHORITIES

At law, we are required to assist law enforcement agencies. Accordingly, 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).

For more information on how we handle Customer information, please refer to our Privacy Policy, https://www.commander.com.au/privacy-policy.

## 6. LAWFUL USE

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.

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. Accordingly, Customers must proactively minimise unlawful or harmful material or activity on a Service (including any encrypted Service).

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 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 child pornography.

## 7. MONITORING COMPLIANCE

We may from time to time monitor transmissions of published content for the purposes of ensuring compliance with this Policy.

## 8. WHAT HAPPENS IF I BREACH THIS POLICY?

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.

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

a) suspend access to the Service indefinitely or for a specific period;
b) terminate access to the Service and refuse to provide the Service to the Customer or their associates in the future;
c) inform appropriate government and regulatory authorities of suspected illegal or infringing conduct;
d) delete or edit any of the Customer's data (including webpage content) stored on systems;
e) override any attempt by the Customer to breach this Policy, such as specify a particular traffic routing pattern; and
f) take any other action we deem appropriate, including taking action against offenders to recover the costs and expenses of identifying them.

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

Please note, our right to suspend access to Services **without notice** under this Policy overrides any requirement our may have to give notice under the relevant Standard Form of Agreement.

## 9. CHANGES

We may vary this Policy from time to time but will do so in line with the relevant notice provisions in your agreement with us.

Continued use of Services after receiving notice once the variation takes effect will constitute acceptance of the variation.

## 10. REPORT A BREACH

You can report a suspected breach of this Policy by sending an email to Retail.Compliance@vocus.com.au.