

Fair Use Policy

Rules for accessing and using the GTE website, online content, forms, customer portals and linked services.

Legal entity	Green Triangle Electronics Pty Ltd
ABN	43 008 187 497
Effective date	1st July 2026
Applies to	Internet, data, fixed voice, VoIP, mobile, failover and related telecommunications services supplied by Green Triangle Electronics (GTE)
Contact	(08) 8724 2222 policies@gte.com.au gte.com.au

This policy forms part of the agreement under which GTE supplies a Service. It applies to the Customer and every person who uses a Service through the Customer's account, equipment or connection.

1. Purpose

GTE wants customers to be able to use its Services reliably, lawfully and safely. This policy sets reasonable rules to:

- protect customers, other users, GTE personnel and the public;
- protect the security, reliability, capacity and reputation of GTE, its networks and its suppliers;
- prevent unlawful, fraudulent, harmful or unreasonable use; and
- explain the action GTE may take when use of a Service breaches this policy.

This policy supplements the Customer's service agreement, order, service schedule, Critical Information Summary and any service-specific terms. If there is an inconsistency, the more specific service term applies to the extent of that inconsistency, subject to applicable law.

2. Definitions

Customer means the person or organisation that acquires a Service from GTE.

GTE, we, us or our means Green Triangle Electronics and any related entity that supplies or supports the relevant Service.

Network means the equipment, systems, infrastructure and networks used to provide a Service, including infrastructure operated by GTE, nbn co, carriers, wholesalers and other suppliers.

Service means any internet, broadband, Ethernet, data, fixed voice, VoIP, mobile, mobile broadband, failover or related telecommunications service supplied by GTE.

Supplier means a carrier, wholesaler, network operator, platform provider or other third party used by GTE to supply or support a Service.

User means the Customer and any employee, contractor, guest or other person who accesses or uses a Service through the Customer's account, premises, SIM, device or equipment.

3. Customer responsibility

The Customer is responsible for all use of a Service through its account, premises, SIMs, devices and equipment, whether or not that use was specifically authorised. The Customer must:

- ensure that Users comply with this policy;
- keep account credentials, security information, SIMs, devices and network equipment secure;
- use reasonable security controls appropriate to the Service and the Customer's environment;
- promptly tell GTE if the Customer suspects unauthorised use, compromise, theft or loss; and
- cooperate with reasonable steps requested by GTE to investigate or stop misuse, a security threat or network harm.

The Customer must not avoid, bypass or attempt to defeat any restriction, security control, traffic-management measure, usage control or suspension applied by GTE or a Supplier.

4. Lawful and respectful use

A Service must not be used, or allowed to be used, to:

- commit, facilitate, encourage or conceal an unlawful, criminal, fraudulent or deceptive act;
- threaten, stalk, harass, intimidate or seriously abuse another person, including GTE personnel;
- create an unreasonable risk to a person's health, safety or property;

- access, store, transmit, publish or distribute material that is unlawful, including illegal or restricted online content;
- infringe another person's intellectual property, privacy, confidentiality or other legal rights;
- impersonate another person or organisation, falsify identity or account information, or misrepresent the origin of a communication; or
- breach any law, court order, regulatory requirement or binding direction that applies to the Customer or the use of the Service.

5. Security and network integrity

A Service must not be used in a way that compromises or attempts to compromise the security, operation or availability of any system, network, service or data. Prohibited activities include:

- gaining or attempting to gain unauthorised access to a system, account, network, device or data;
- probing, scanning or testing a system or network that the User does not own or does not have express authority to test;
- introducing, distributing or controlling malware, ransomware, spyware, botnets, malicious code or harmful files;
- launching or participating in denial-of-service attacks, flooding, traffic amplification, resource exhaustion or similar activity;
- forging or manipulating packet headers, sender details, caller identification, domain information or routing information for a deceptive or improper purpose;
- operating an open mail relay, open proxy, open recursive resolver or similar system where it is being used to cause abuse or network harm;
- interfering with, damaging, modifying or bypassing GTE or Supplier equipment, network termination equipment, security controls or service configuration; or
- using a Service in a way that causes, or is reasonably likely to cause, disruption, congestion, degradation, excessive signalling, abnormal load or other material harm to the Network or other users.

6. Spam and automated communications

The Customer must not use a Service to send, enable or assist spam, phishing, scam communications or other unsolicited communications contrary to applicable law. This includes email, SMS, MMS, instant messages, voice calls and fax communications. Where the Customer sends commercial electronic messages, telemarketing calls or other bulk communications, the Customer must be able to demonstrate that it has all required consent, identification, unsubscribe, calling-time and record-keeping arrangements.

The Customer must not:

- use purchased, harvested, generated or unlawfully obtained contact lists;
- continue sending messages or making calls after consent has been withdrawn or a valid opt-out request has been made;
- use false, misleading or concealed sender information or caller identification;
- operate phishing campaigns, scam campaigns, robocalling, fax broadcasting or bulk messaging that is unlawful or not expressly supported by the Service; or
- allow a device, account or system compromised by a third party to continue sending harmful or unsolicited communications after becoming aware of the issue.

7. Reasonable and ordinary use

A reference to "unlimited" usage means that the plan does not have a stated fixed usage allowance or automatic excess-usage charge. It does not permit unrestricted use and remains subject to this policy, the service description and any technical limitations. High usage by itself is not necessarily a breach. GTE may treat use as unreasonable where, having regard to the type and purpose of the Service, the use:

- materially and adversely affects the availability, performance or security of the Network or another customer's service;
- is persistently or substantially inconsistent with the ordinary purpose, configuration or customer type for which the Service is supplied;
- involves automated, continuous or excessive activity that creates unusual network load, risk or third-party cost;
- is principally intended to resell, aggregate, arbitrage or commercially exploit inclusions intended for the Customer's own use;
- continues after GTE has reasonably asked the Customer to change or reduce the activity; or
- causes GTE to breach, or creates a material risk that GTE will breach, a Supplier requirement or applicable law.

When deciding whether use is unreasonable, GTE will consider the nature, volume, pattern, duration and impact of the use, the plan and Service involved, whether the activity was intentional, the Customer's previous conduct and the Customer's response to any request to address the issue.

8. Service-specific requirements

8.1 Broadband, Ethernet and data services

Unless GTE agrees otherwise in writing, the Customer must not:

- use one connection to supply or serve more than one physical premises;
- resell, wholesale, redistribute or provide public access to the Service for payment;

- connect or use equipment that is unlawful, unsafe, incompatible or likely to damage or interfere with the Network;
- interfere with, relocate, alter or bypass carrier or nbn network termination equipment; or
- use a mobile or fixed-wireless failover Service as a permanent primary connection once the relevant primary fixed service is reasonably available, unless the plan expressly allows that use.

8.2 Fixed voice and VoIP services

Unless the plan or order expressly supports the activity, voice inclusions are intended for ordinary person-to-person or ordinary business communications. The Customer must not use a voice Service for:

- call-centre, predictive-dialler, auto-dialler, continuous-dialling, fax-broadcast or mass-telemarketing activity;
- traffic pumping, number farming, call arbitrage, artificial call generation or activity designed mainly to obtain a payment, rebate, credit or other benefit;
- operating a conferencing platform, calling-card service, gateway, switch or call-rerouting service for third parties;
- bypassing call caps, interconnection charges, routing controls or service restrictions; or
- persistent call forwarding or machine-to-machine use that is materially inconsistent with the plan's intended purpose.

8.3 Mobile and mobile broadband services

Unless GTE agrees otherwise in writing, the Customer must not:

- use a SIM in a SIM box, GSM gateway, fixed cellular terminal or similar device for call termination, traffic aggregation or resale;
- aggregate or combine traffic for multiple unrelated customers or premises;
- use automated processes to generate unusually high numbers of calls, messages, sessions or signalling events;
- use a mobile failover service as a permanent primary service contrary to its stated purpose; or
- use the Service in a way that breaches a mobile network operator's reasonable and lawful requirements notified to the Customer.

9. Wholesale and supplier requirements

Some Services are supplied using networks, products or platforms provided by Suppliers. The Customer must comply with reasonable and lawful technical, security and acceptable-use requirements that apply to the Service and that GTE notifies to the Customer.

GTE may take action under this policy where a Supplier reasonably identifies misuse, network harm or a breach affecting the Service, or directs GTE to restrict, suspend or terminate access. GTE will not impose a Supplier requirement that is inconsistent with mandatory law or the Customer's express contractual rights.

10. Network protection and management

GTE may take reasonable technical and operational measures to protect the Network, customers and Suppliers. Depending on the circumstances, these measures may include filtering malicious traffic, blocking known threats, limiting particular traffic, rate-limiting, changing routing, isolating a compromised device or connection, or temporarily restricting a feature or Service.

GTE will use these measures only where reasonably necessary for security, network integrity, legal compliance, Supplier compliance or fair access to shared network resources. Any management of a Service remains subject to the service agreement and applicable law.

11. Investigation and action

Where GTE reasonably suspects a breach, it may investigate using account, network, security and usage information available to it, in accordance with its Privacy Policy and applicable law. GTE may ask the Customer to provide information or take corrective action. GTE will generally take action that is proportionate to the nature, seriousness and urgency of the issue. Action may include:

- contacting the Customer and requesting an explanation or corrective action;
- giving guidance, a warning or a reasonable period to remedy the breach;
- blocking or filtering particular traffic, destinations, ports, numbers, messages or features;
- restricting, shaping, isolating or suspending all or part of a Service;
- refusing to restore a Service until the risk or breach has been adequately addressed;
- terminating the affected Service or agreement in accordance with its terms; and
- referring or disclosing information to a Supplier, regulator, law-enforcement agency or other authority where required or permitted by law.

Where reasonably practicable, GTE will give notice and an opportunity to remedy before restricting, suspending or terminating a Service. GTE may act immediately and without prior notice where necessary to address an urgent security threat, serious network harm, suspected unlawful conduct, risk to another person, a binding legal requirement or an urgent Supplier direction.

12. Review and complaints

A Customer who believes action under this policy is incorrect or disproportionate may ask GTE to review the decision. The Customer should provide any relevant information showing why the use was authorised, lawful, secure and consistent with the Service.

Complaints will be handled under GTE's Complaints Handling Policy. The Customer may also have rights under applicable telecommunications or consumer law and, where eligible, access to an external dispute-resolution body.

13. Changes to this policy

GTE may update this policy from time to time to reflect changes to Services, networks, Supplier requirements, technology, security threats or law. GTE will publish the current version and give any notice required by the Customer's agreement or applicable law before a material adverse change takes effect.

14. Contact

Questions, suspected misuse and review requests should be directed to:

Green Triangle Electronics

169-171 Commercial Street West

Mount Gambier, S.A 5290

Postal address: P.O. Box 2548

Telephone: 08 87242222

Email: policies@gte.com.au

Website: <https://www.gte.com.au>