Acceptable Use Policy

Lawful, safe and secure use of GTE telecommunications, internet, voice, mobile, hosted, cloud and related services

Legal entity	Green Triangle Electronics Pty Ltd
ABN	43 008 187 497
Effective date	1st July 2026
Applies to	Customers and Users of GTE Services
Contact	(08) 8724 2222 | policies@gte.com.au | gte.com.au

About this policy

This Acceptable Use Policy sets the rules for lawful, safe and secure use of Services supplied by Green Triangle Electronics Pty Ltd (GTE). It forms part of the agreement under which GTE supplies a Service and applies to the Customer and every person who accesses or uses a Service through the Customer's account, premises, equipment, SIM, device, credentials or connection.

Relationship with the Fair Use Policy
This policy applies to unlawful, harmful, abusive, fraudulent or insecure use of a Service. GTE's Fair Use Policy separately applies to excessive or unreasonable use, unusual network load, and use inconsistent with the intended purpose of a plan

Nothing in this policy excludes, restricts or modifies a right, guarantee, remedy or protection that cannot legally be excluded. If this policy conflicts with mandatory law, mandatory law prevails.

1. Purpose and scope

1.1 The purpose of this policy is to protect Customers, Users, GTE personnel, suppliers, networks, systems, data and the public from unlawful, harmful, abusive, fraudulent or insecure use of a Service.

1.2 This policy applies to internet, nbn®, fixed wireless, Ethernet, data, fixed voice, VoIP, mobile, mobile broadband, failover, hosted, cloud and related services supplied or supported by GTE, unless a service-specific document states otherwise.

1.3 This policy is read with the applicable Service Order, Critical Information Summary, Telecommunications Customer Terms and Conditions, Fair Use Policy, Privacy Policy and any service-specific terms. More specific terms prevail to the extent of an inconsistency, subject to mandatory law.

1.4 This policy does not prohibit legitimate security testing, network administration, research or other technical activity carried out by an authorised person within an expressly approved scope and in compliance with law.

2. Definitions

Customer: the person, business, government body, not-for-profit organisation or other entity that acquires or uses a Service from GTE.

Customer Equipment: equipment, devices, systems, software, networks, routers, handsets, servers or cabling owned or controlled by the Customer.

GTE, we, us or our: Green Triangle Electronics Pty Ltd, ABN 43 008 187 497

Network: the systems, equipment, platforms and networks used to provide or support a Service, including those operated by GTE, carriers, wholesalers, NBN Co and other suppliers.

Service: a service within clause 1.2 and any associated account, number, SIM, credential, IP address, hosted resource or feature.

Supplier: a carrier, wholesaler, network operator, platform provider, data centre, cloud provider, software provider or contractor used by GTE to supply or support a Service.

User: the Customer and any employee, contractor, guest, end user or other person who accesses or uses a Service through the Customer.

3. Customer and User responsibilities

3.1 The Customer must take reasonable steps to ensure that all Users comply with this policy and must manage use of the Service in accordance with the Customer's agreement and applicable law.

3.2 The Customer must:

- keep account credentials, PINs, SIMs, eSIM profiles, devices, systems and network equipment reasonably secure;

- use security controls appropriate to the Service, the Customer's environment and reasonably foreseeable risks;
- keep software, operating systems, applications and security tools appropriately maintained where they are the Customer's responsibility;
- promptly notify GTE of suspected unauthorised use, fraud, compromise, theft, loss, malware or a material security incident affecting a Service;
- cooperate with reasonable, proportionate steps requested by GTE to investigate, contain or remediate misuse, fraud, a security threat or network harm; and
- maintain accurate authorised-contact details and promptly revoke access for people who no longer require it.

3.3 The Customer and Users must not bypass or attempt to defeat a lawful restriction, security control, usage control, fraud control, traffic-management measure, block, quarantine or suspension applied by GTE or a Supplier.

4. Lawful and respectful use

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

- commit, facilitate, encourage, conceal or profit from an unlawful, criminal, fraudulent, deceptive or seriously harmful act;
- impersonate another person or organisation, falsify identity or authority information, or misrepresent the origin of a communication for an improper purpose;
- threaten, stalk, harass, intimidate, coerce or seriously abuse another person, including GTE personnel;
- publish, distribute or threaten to distribute intimate images or other private material without lawful authority or consent;
- create an unreasonable risk to a person's health, safety, property, privacy or security;
- interfere with emergency services, make hoax emergency communications or misuse an emergency number;
- breach a court order, regulatory direction, sanctions requirement or other binding legal obligation; or
- assist another person to engage in conduct prohibited by this policy.

4.2 GTE may require abusive, threatening or unsafe communications with GTE personnel to occur through a nominated contact or written channel, provided this does not prevent access to emergency help, payment assistance, complaints processes or other rights required by law.

5. Illegal and restricted content

5.1 A Service must not be used to access, store, host, transmit, publish, promote, solicit or distribute content where doing so is unlawful. This includes content involving child sexual abuse or exploitation, pro-terror material, abhorrent violent conduct, non-consensual intimate images, or other illegal or restricted content regulated under Australian law.

5.2 A Customer must not use a Service to operate a platform, repository, website or distribution system that knowingly facilitates unlawful content or deliberately defeats a lawful access restriction, removal notice, blocking direction or age-access requirement.

5.3 This clause does not prohibit lawful possession or handling of material by an authorised law-enforcement body, regulator, legal adviser, researcher, security professional or other person acting within lawful authority and appropriate safeguards.

6. Security and network integrity

6.1 A Service must not be used in a way that compromises, damages or attempts to compromise or damage any system, account, network, device, service or data. Prohibited activities include:

- gaining or attempting to gain access without authorisation;
- probing, scanning, enumerating, testing or exploiting a system or network without express authority from the owner or responsible operator;
- introducing, distributing, controlling or knowingly hosting malware, ransomware, spyware, credential-stealing tools, botnets, malicious code or harmful files;
- launching, assisting or participating in denial-of-service attacks, traffic amplification, flooding, resource exhaustion or similar activity;
- intercepting communications or data without lawful authority;
- forging or manipulating packet headers, sender information, caller identification, domain information, routing information or authentication data for a deceptive, fraudulent or harmful purpose;
- operating an open mail relay, open proxy, open recursive resolver or similar service that is causing or is reasonably likely to cause abuse or network harm;
- interfering with, damaging, modifying, relocating or bypassing GTE or Supplier equipment, network termination equipment, security controls or service configuration; or
- using a Service in a manner that causes, or is reasonably likely to cause, a material security risk, service disruption, abnormal signalling or harm to the Network or other users.

6.2 Where a Customer becomes aware that Customer Equipment or a User account has been compromised, the Customer must take reasonable steps to contain the incident and prevent continuing misuse. GTE may assist under the applicable support arrangement, and additional remediation work may be chargeable where agreed.

7. Spam, telemarketing and automated communications

7.1 A Customer must not use a Service to send, enable, assist or profit from spam, phishing, scam communications or unlawful unsolicited communications. This includes email, SMS, MMS, instant messaging, fax and voice communications.

7.2 A Customer conducting commercial messaging, telemarketing, research calls or other bulk communications must comply with all applicable consent, identification, unsubscribe, calling-time, contact-list, Do Not Call Register and record-keeping requirements.

7.3 The Customer must not:

- use purchased, harvested, generated, scraped or unlawfully obtained contact lists without a lawful basis and required consent;
- continue messaging or calling after consent has been withdrawn or a valid unsubscribe or opt-out request has taken effect;
- use false, misleading or concealed sender information, caller identification or business identity;
- conduct phishing, scam, unlawful robocalling, fax broadcasting, spoofing or bulk messaging campaigns;
- use a Service for artificial traffic generation, traffic pumping, number farming or activity designed mainly to obtain a rebate payment, credit or other improper benefit; or
- allow a compromised device, account or system to continue sending harmful or unsolicited communications after becoming aware of the issue.

8. Privacy, confidentiality and intellectual property

8.1 A Customer and User must not use a Service to unlawfully collect, access, use, disclose, sell, publish or interfere with another person's personal information, confidential information, trade secrets or credentials.

8.2 A Service must not be used to infringe copyright, trade marks, patents, moral rights, database rights or other intellectual property rights, including by knowingly distributing unauthorised copies or operating a service primarily designed to facilitate infringement.

8.3 GTE may respond to a properly substantiated infringement notice, court order or lawful direction by seeking information, preserving records, restricting access or taking other action permitted or required by law. GTE does not determine private legal disputes merely because an allegation is made.

9. Service-specific requirements

9.1 *Internet, broadband, Ethernet and data services*

- The Customer must not resell, wholesale, redistribute or provide public access to a Service for payment unless the Service Order expressly permits it.
- The Customer must not connect equipment that is unlawful, unsafe, incompatible or reasonably likely to damage or interfere with the Network.
- The Customer must not alter, relocate, remove or bypass carrier or NBN Co network termination equipment except through an authorised process.
- Use of static IP addresses, servers, public-facing systems or remote-access services must be appropriately secured by the Customer unless GTE has expressly agreed to manage that security.

9.2 *Voice and messaging services*

- Voice or messaging Services must not be used for unlawful call-centre, predictive-dialler, auto-dialler, continuous-dialling, mass-telemarketing or fax-broadcast activity.
- The Customer must not operate a calling-card service, gateway, switch, call-rerouting service, conferencing platform or message aggregation service for third parties unless expressly approved.
- The Customer must not bypass call caps, interconnection charges, routing controls, authentication, service restrictions or number-use requirements.

9.3 *Mobile and mobile broadband services*

- A SIM or eSIM must not be used in a SIM box, GSM gateway, fixed cellular terminal or similar device for call termination, traffic aggregation, artificial traffic or resale unless expressly approved.
- The Customer must not generate abnormal volumes of automated calls, messages, sessions, location updates or signalling events that create fraud, security or network risk.
- A mobile failover Service must not be used contrary to a clearly disclosed service purpose or Supplier requirement.

9.4 *Hosted, cloud and managed services*

- The Customer must not knowingly host or distribute malicious code, phishing infrastructure, credential theft tools, unlawful content or attack infrastructure.
- The Customer must not use shared computing, storage or network resources for unauthorised cryptocurrency mining, password cracking, bulk scanning or other resource-intensive activity outside the agreed service purpose.

- Administrative access, API keys, service accounts and privileged credentials must be protected and used only by authorised people and systems.

- Where GTE manages a service, the Customer must not make unauthorised changes that materially undermine agreed security, backup, monitoring or support controls.

9.5 *Supplier requirements*
Some Services use Supplier networks or platforms. The Customer must comply with reasonable and lawful technical, security and acceptable-use requirements that apply to the Service and that GTE provides or makes reasonably available. A Supplier requirement does not override mandatory law or an express Customer right.

10. Reporting suspected misuse

10.1 A Customer or third party may report suspected misuse, spam, fraud, security incidents or policy breaches to GTE using the contact details in clause 15. Reports should include enough information for GTE to identify the affected Service or activity, such as dates, times, numbers, IP addresses, message headers, screenshots or logs, but should not include passwords or unnecessary sensitive information.

10.2 If a person is in immediate danger, they should contact Triple Zero (000). Illegal or restricted online content may also be reported to the eSafety Commissioner, and suspected criminal conduct may be reported to police.

10.3 GTE may be unable to provide the reporting person with detailed investigation outcomes because of privacy, confidentiality, security or legal restrictions.

11. Investigation, network protection and privacy

11.1 GTE does not undertake to routinely inspect or monitor the content of all communications. However, where permitted by law, GTE may use service, account, network, security, traffic and usage information available to it to operate and protect Services, investigate a specific report or suspected breach, respond to a Supplier or regulator, and comply with legal obligations.

11.2 GTE may take reasonable technical and operational measures to protect people, Services, networks and systems. These measures may include filtering known malicious traffic, blocking known threats or destinations, rate-limiting, changing routing, disabling a compromised credential, isolating a device or connection, or temporarily restricting a feature.

11.3 GTE will handle information obtained or used under this policy in accordance with its Privacy Policy, confidentiality obligations and applicable law. GTE may preserve or disclose information where required or permitted by law, including to a Supplier, regulator, emergency service, law-enforcement agency or court.

11.4 This policy does not create a guarantee that GTE will detect, prevent or remove every instance of misuse, malicious traffic or unlawful content.

12. Action GTE may take

12.1 Where GTE reasonably believes that a breach has occurred or that urgent action is required to protect a person, a Service, a Network or a system, GTE may take action that is reasonable and proportionate to the nature, seriousness, impact and urgency of the issue.

12.2 Action may include:

- contacting the Customer and requesting information, an explanation or corrective action;
- giving guidance, a warning or a reasonable opportunity to remedy the issue;
- requiring the Customer to secure, disconnect, patch, reconfigure, replace or remove affected Customer Equipment or credentials;
- blocking or filtering particular traffic, destinations, ports, numbers, messages, features or content where technically and legally appropriate;
- rate-limiting, isolating, restricting or suspending all or part of an affected Service;
- refusing to restore a Service until the relevant risk or breach has been adequately addressed;
- terminating the affected Service in accordance with the Agreement and applicable law; or
- referring or disclosing information to a Supplier, regulator, emergency service, law-enforcement agency or other authority where required or permitted by law.

12.3 Where reasonably practicable, GTE will provide notice and an opportunity to remedy before restricting, suspending or terminating a Service. GTE may act without prior notice where immediate action is reasonably necessary for safety, security, fraud prevention, serious network harm, emergency services, suspected serious unlawful conduct, a binding legal requirement or an urgent lawful Supplier direction.

12.4 GTE will review an urgent restriction or suspension as soon as reasonably practicable and will restore the Service when the material risk has been addressed, subject to the Agreement, Supplier requirements and applicable law.

12.5 GTE will not use this policy to avoid a non-excludable obligation, penalise a Customer merely for making a complaint, or take action that is unfair, arbitrary or disproportionate.

13. Review and complaints

13.1 A Customer who believes that action under this policy is incorrect or disproportionate may ask GTE to review the decision and may provide relevant information showing why the activity was authorised, lawful, secure or adequately remediated.

13.2 Complaints will be handled under GTE's Complaints Handling Policy. Making a complaint does not remove any immediate obligation to stop activity that creates an urgent safety, security or network risk.

13.3 An eligible telecommunications customer may have access to the Telecommunications Industry Ombudsman after giving GTE a reasonable opportunity to resolve the complaint.

14. Changes to this policy

14.1 GTE may update this policy to reflect changes to Services, networks, Supplier requirements, technology, security threats, law or operational processes.

14.2 The current version will be published on GTE's website. GTE will give any notice required by the Customer's Agreement or applicable law before a material adverse change applies to an existing Service.

15. Contact and reference framework

Organisation	Green Triangle Electronics Pty Ltd
Address	169-171 Commercial Street West, Mount Gambier SA 5290
Telephone	(08) 8724 2222
Email	policies@gte.com.au
Website	gte.com.au

Related GTE documents:

- Telecommunications Customer Terms and Conditions
- Fair Use Policy
- Privacy Policy
- Complaints Handling Policy
- Critical Information Summary and service-specific terms

Reference framework

This policy is intended to operate consistently with applicable Australian law, including the Telecommunications Act 1997, Telecommunications (Interception and Access) Act 1979, Spam Act 2003, Do Not Call Register Act 2006, Online Safety Act 2021, Privacy Act 1988, Copyright Act 1968, Competition and Consumer Act 2010 and Australian Consumer Law. If there is an inconsistency, applicable law prevails.