

POLICY

Acceptable Use Policy

VERSION
v2026.10cEFFECTIVE
1 November 2026REPLACES
Acceptable-Use-Policy-Updated.pdf

1. Status and purpose

- 1.1 This Acceptable Use Policy ("AUP") applies to every customer of FirstNet Technology Services (Pty) Ltd ("FirstNet") and to every person who uses a FirstNet service through a customer's account ("User"). It forms part of the customer's agreement with FirstNet (the FirstNet Standard Terms and Conditions or the customer's signed Master Services Agreement, the "Agreement"). Words defined in the Agreement have the same meanings here.
- 1.2 This AUP sets out what is not acceptable use of FirstNet's network, platforms and services, so that FirstNet can comply with South African law, protect its network and other customers, and explain what it may do if the AUP is breached.
- 1.3 Use of the FirstNet website is governed by FirstNet's Website Terms of Use, not by this AUP.
- 1.4 FirstNet respects the rights of its customers and Users to freedom of expression, access to information, privacy and dignity under the Constitution. FirstNet will not interfere with those rights unless required by law, unless they are exercised unlawfully, or unless their exercise threatens harm to others or the integrity of FirstNet's network.
- 1.5 The customer is responsible for all use of its services, including by its Users, and must make sure that its Users know about and follow this AUP.

2. ISPA membership and Code of Conduct

- 2.1 FirstNet is a member of the Internet Service Providers' Association ("ISPA"), the Industry Representative Body recognised under section 71 of the Electronic Communications and Transactions Act 25 of 2002 ("ECTA"), and is bound by the ISPA Code of Conduct, available at <https://ispa.org.za/membership/code-of-conduct/>.
- 2.2 Complaints about FirstNet's compliance with the ISPA Code of Conduct may be made to ISPA under its complaints procedure at <https://ispa.org.za/consumer-support/complaints-process/>.

3. Unlawful use

- 3.1 FirstNet's services may only be used for lawful purposes. Customers and Users must not use any FirstNet service to create, store, transmit, publish or distribute material, or to carry out any activity, that breaches South African law or the law of any other country that applies. This includes:
 - 3.1.1 creating, possessing, distributing or providing access to child sexual abuse material, as defined in the Films and Publications Act 65 of 1996, including material generated or altered by artificial intelligence, or any content that sexually exploits children;
 - 3.1.2 distributing intimate images of a person without their consent, or harmful data messages that incite violence, threaten persons or property, or are prohibited by Chapter 3 of the Cybercrimes Act 19 of 2020;
 - 3.1.3 hate speech, incitement to violence, unfair discrimination, harassment, stalking, threats or defamation;
 - 3.1.4 infringing copyright, trade marks, trade secrets or other intellectual property, including distributing pirated software, films or music;
 - 3.1.5 fraud, phishing, identity theft, impersonation, pyramid or other unlawful investment schemes, and any attempt to transact with FirstNet in another person's name without their authority;
 - 3.1.6 collecting or processing personal information unlawfully or in breach of the Protection of Personal Information Act 4 of 2013 ("POPIA"), including harvesting email addresses or phone numbers without consent;

- 3.1.7 intercepting or monitoring communications in breach of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("RICA");
- 3.1.8 any offence under the Cybercrimes Act 19 of 2020, including unlawful access, interception of data, interference with data or computer systems, cyber fraud, cyber forgery and cyber extortion; and
- 3.1.9 breaching exchange control, sanctions or export control laws.

4. Network and system security

- 4.1 Customers and Users must not do anything that threatens the operation, security or integrity of FirstNet's network or any other network or system, including:
 - 4.1.1 accessing, or attempting to access, any system, network, account or data without authorisation, or bypassing authentication or security measures ("hacking");
 - 4.1.2 scanning, probing or testing the vulnerability of a system or network without the owner's written authorisation (authorised penetration testing of the customer's own systems is allowed if FirstNet is told in advance where it may affect FirstNet's network);
 - 4.1.3 denial-of-service attacks, flooding, or deliberately overloading a service or network;
 - 4.1.4 forging or spoofing IP packet headers, email headers, caller line identification or any other identifying information;
 - 4.1.5 distributing or hosting malware, including viruses, worms, Trojans, ransomware, spyware and botnet command-and-control infrastructure;
 - 4.1.6 monitoring data or traffic on FirstNet's network without FirstNet's written consent;
 - 4.1.7 operating open mail relays, open DNS resolvers, open proxies or other services that can be abused by third parties, after FirstNet has asked the customer to secure them; and
 - 4.1.8 using IP addresses that FirstNet has not assigned to the customer, or announcing routes the customer is not authorised to announce.

5. Email, messaging and marketing

- 5.1 Customers and Users must not send unsolicited electronic communications in breach of section 69 of POPIA or section 45 of ECTA. In particular:
 - 5.1.1 electronic direct marketing (email, SMS, WhatsApp and similar messages, and automated calls) may only be sent to a person who has given prior consent, or to an existing customer about similar products or services under section 69(3) of POPIA;
 - 5.1.2 every marketing message must identify the sender and give a free way to opt out, and opt-out requests must be honoured promptly;
 - 5.1.3 mailing lists may not be bought, harvested or used without the consent of the people on them;
 - 5.1.4 FirstNet's name, domain names or IP addresses may not be used in the headers of unsolicited messages, whether or not they are sent through FirstNet's network; and
 - 5.1.5 FirstNet's services may not be used to collect replies to unsolicited messages sent through another provider.
- 5.2 Customers who run their own mail servers must secure them against open relay. FirstNet may test a customer's mail server, or a server that relays mail through FirstNet ("smarthosting"), to check that it is not an open relay, and will share the results with the customer.

6. Voice services

- 6.1 Customers and Users of FirstNet voice services must not:
 - 6.1.1 use the services for robocalling, auto-dialled marketing calls or bulk messaging without the consent required by section 69 of POPIA and any applicable code;

- 6.1.2 spoof, hide or misrepresent caller line identification (CLI), or present a number the customer is not authorised to use;
 - 6.1.3 generate artificial traffic, such as traffic pumping, wangiri (missed-call fraud) or calls designed to inflate termination revenue;
 - 6.1.4 use SIM boxes or other equipment to re-originate calls in a way that breaches interconnection or licensing rules;
 - 6.1.5 record or monitor calls other than as allowed by RICA (for example where a party to the call has consented, or in the course of business with notice under section 6 of RICA), and must give callers the notices required by law; or
 - 6.1.6 use call branding or business caller identification services (such as Truecaller for Business) to misrepresent who is calling.
- 6.2 The customer is responsible for securing its PBX, handsets, softphones and SIP credentials against unauthorised use (toll fraud). FirstNet may block destinations or suspend a service where it detects suspicious calling patterns.

7. Cloud, hosting and colocation services

- 7.1 Customers and Users of FirstNet cloud, hosting, colocation and backup services must not:
- 7.1.1 host phishing sites, malware, command-and-control servers, illegal content or content that infringes intellectual property;
 - 7.1.2 use compute resources for cryptocurrency mining unless FirstNet has agreed to it in writing;
 - 7.1.3 run services that are exposed to abuse (such as open resolvers, open proxies or unauthenticated databases) after being asked to secure them;
 - 7.1.4 use the services to store or distribute content in breach of section 3; or
 - 7.1.5 resell or sublet hosting or colocation space without FirstNet's written consent.
- 7.2 Customers hosting websites or applications are responsible for patching and securing them. Compromised sites that are being used to attack others may be suspended until they are cleaned.

8. AI services

- 8.1 Customers and Users of FirstNet AI services (including FirstCoreAI GPU, inference, engineering, content and assistant services) must not use them to:
- 8.1.1 generate or attempt to generate child sexual abuse material, or any sexual content involving minors;
 - 8.1.2 create intimate or sexual images of a real person, or realistic images, video or voice of a real person ("deepfakes"), without that person's consent, or to deceive others about what a real person said or did;
 - 8.1.3 create malware, exploit code for unauthorised use, or tools for fraud, phishing or impersonation;
 - 8.1.4 generate disinformation intended to deceive the public, election interference or content that incites violence or hatred;
 - 8.1.5 make decisions with legal or similarly significant effects on individuals based solely on automated processing, without human oversight and the measures required by section 71 of POPIA;
 - 8.1.6 process personal information without a lawful basis, or process special personal information or children's personal information without the authorisations POPIA requires;
 - 8.1.7 infringe the intellectual property or other rights of third parties, or breach the licence or acceptable use terms of the underlying model; or
 - 8.1.8 attempt to extract model weights, training data or other customers' data, bypass safety controls or rate limits, or overload the AI Factory.
- 8.2 Customers must tell people when they are interacting with an AI system where a reasonable person would not otherwise know, and must label AI-generated images, audio or video of real people where it could mislead.

9. Fair use

- 9.1 Some services are subject to fair use rules (for example the FirstNet Broadband Fair Use Policy for uncapped broadband, fibre and LTE). Customers must comply with the fair use rules for their service, as set out in the Service Specific Terms.

10. Protection of children

- 10.1 FirstNet prohibits the use of its services to harm or attempt to harm a child, including by creating, hosting, possessing, distributing or providing access to child sexual abuse material.
- 10.2 As required by section 27A of the Films and Publications Act 65 of 1996, FirstNet takes all reasonable steps to prevent the use of its services for hosting or distributing child sexual abuse material, and, if it becomes aware that its services are being used for that purpose, will report it to the South African Police Service with the particulars of the person concerned, preserve the evidence for investigation, and take steps to prevent access to the material.
- 10.3 Where a customer allows a child to use a FirstNet service, the customer (as parent, guardian or employer) is responsible for that child's online conduct and for controlling the child's access. ISPA publishes guidance on parental controls and safe use at <https://ispa.org.za/consumer-support/for-children-and-teens/>.

11. Duties under the Cybercrimes Act

- 11.1 Where FirstNet becomes aware that its network or services are involved in an offence of the kind described in section 54 of the Cybercrimes Act 19 of 2020, FirstNet will, as that section requires once in force, report the offence to the South African Police Service within 72 (seventy-two) hours and preserve any information that may help with the investigation.

12. Law enforcement and lawful requests

- 12.1 FirstNet complies with interception directions, requests for communication-related information and other lawful requests issued under RICA, the Criminal Procedure Act 51 of 1977, the Cybercrimes Act and other South African law.
- 12.2 FirstNet will assist foreign law enforcement agencies only through South African legal processes, such as a mutual legal assistance request or a South African court order, and will disclose only the information that the process requires.

13. Notice and take-down

- 13.1 Under section 75 of ECTA, FirstNet has designated ISPA as its agent to receive notifications of unlawful activity (take-down notices) under section 77 of ECTA. Take-down notices must be sent to ISPA using the details and form on ISPA's website:
- 13.1.1 Internet Service Providers' Association NPC (ISPA);
 - 13.1.2 telephone: 010 500 1200;
 - 13.1.3 email: queries@ispa.org.za;
 - 13.1.4 take-down procedure: <https://ispa.org.za/consumer-support/take-down-notice/>, and online form: <https://ispa.org.za/consumer-support/take-down-notice/take-down-form/>.
- 13.2 FirstNet may remove or disable access to material in response to a valid take-down notice, as permitted by Chapter XI of ECTA, and is not liable to the customer for doing so in good faith. A person who submits a take-down notice that contains material misrepresentations may be liable for damages under section 77(2) of ECTA.

14. Reporting abuse

- 14.1 To report spam, network abuse or unlawful content coming from the FirstNet network, email abuse@firstnet.co.za with as much detail as possible (including full email headers, IP addresses, timestamps with time zone, and URLs).

- 14.2 To report child sexual abuse material, you may also report it directly to the Film and Publication Board or the South African Police Service. Do not send copies of the material to FirstNet.

15. What FirstNet may do if this AUP is breached

- 15.1 If FirstNet reasonably believes that a customer or User has breached this AUP, FirstNet may, depending on the seriousness of the breach:
- 15.1.1 ask the customer to stop the activity and fix the problem;
 - 15.1.2 block specific traffic, ports, destinations or content;
 - 15.1.3 remove or disable access to content, as allowed by law;
 - 15.1.4 suspend the affected service under clause 17.4 of the Standard Terms and Conditions (or the corresponding clause of a signed Master Services Agreement): without prior notice where reasonably necessary to protect the network, other customers or the customer from a security threat, fraud or unauthorised use, or to comply with the law, a regulator, a court order or a lawful direction; otherwise on notice if the customer does not stop the breach when asked;
 - 15.1.5 terminate the service under the Agreement for serious or repeated breaches;
 - 15.1.6 report the activity to law enforcement, regulators, ISPA or other network operators; and
 - 15.1.7 recover reasonable costs of investigating and remedying the breach.
- 15.2 FirstNet does not routinely monitor the content of customers' communications. FirstNet may monitor traffic volumes, patterns and metadata to protect its network and enforce this AUP, and may investigate the content of communications only where allowed by law.
- 15.3 FirstNet's failure to act on a breach does not waive its right to act on that or any later breach.

16. Third-party content

- 16.1 FirstNet provides access to the internet and does not control the content available on it. Where FirstNet acts as a mere conduit, cache or host, the limitations of liability in sections 73 to 76 of ECTA apply. Customers are responsible for evaluating content they access and for transactions they enter into with third parties online.

17. Changes to this AUP

- 17.1 FirstNet may update this AUP under clause 7 of the Standard Terms and Conditions (or the corresponding clause of a signed Master Services Agreement). FirstNet will publish the updated AUP at www.firstnet.co.za/legal-notices/ and give customers at least 30 (thirty) calendar days' notice of a change that materially and adversely affects them, unless a shorter period is required by law, a regulator or for security reasons. The customer's rights under clause 7.3 of the Standard Terms and Conditions (or the corresponding clause), including the right to end the affected service, apply.

Acceptable Use Policy | Version v2026.10c | Effective date: 1 November 2026

Published by FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07), 26 Augrabies Road, Waterfall Office Park, Midrand, 1686 | 0861 989 896 | support@firstnet.co.za

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. Acceptable Use Policy, v2026.10c. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.