



Foxus Acceptable Use Policy

This Acceptable Use Policy ("Policy") forms part of the agreement between Foxus Pty Ltd (ABN 49 642 695 323) ("Foxus", "we", "us", "our") and all customers or end users ("you", "your") of our services. It sets out rules designed to ensure fair, lawful, and secure use of our mobile, broadband, and related network services. By using our services, you agree to comply with this Policy.

1. Permitted and Lawful Use

You must only use Foxus services for lawful purposes. You must not use our network or systems to:

- Break any applicable law or regulation;
- Infringe intellectual property, trade marks, trade secrets, privacy rights, or publicity rights of others;
- Transmit, distribute, or store offensive, abusive, threatening, or otherwise harmful material;
- Spread malware, viruses, worms, Trojans, or other malicious code.

2. Unsolicited Communications (Spam)

You must not use Foxus services to send or distribute unsolicited bulk messages (including email, SMS, MMS, or group posts). Exceptions apply where:

- Messages comply with Australian spam legislation (e.g. Spam Act 2003 (Cth));
- The recipient has an existing business or personal relationship with you; or
- The recipient has expressly consented to receive such communications.

Any permitted bulk messages must include a clear unsubscribe mechanism that is active and functional.

3. Other Prohibited Activities

You must not use Foxus services to:

- Disguise the source of data, forge headers, or use deceptive addressing;
- Relay messages without permission through another party's mail server;
- Collect or harvest emails, phone numbers, or personal details for unsolicited use;
- Send excessive or disruptive traffic intended to impair another user, device, or service;
- Harass, inconvenience, or cause undue anxiety to others;
- Promote Voice-over-IP (VoIP) or SMS-over-IP services in breach of Foxus' terms.

4. Network and System Security

You must not attempt to breach or interfere with the security of Foxus systems or any connected network. Prohibited actions include:

- Accessing data not intended for you;
- Scanning, probing, or testing vulnerabilities without authorisation;
- Attempting to overload, disrupt, or disable services (e.g. denial-of-service attacks);
- Forging TCP/IP packet headers or similar methods of impersonation.

Breaches may lead to suspension, termination, and possible civil or criminal liability.

5. Malware, Viruses, and Attacks

You are responsible for ensuring your systems are protected against viruses, worms, Trojans, and denial-of-service attacks. We strongly recommend you use up-to-date antivirus, firewalls, and safe email/attachment handling practices.

6. Suspension or Termination

Foxus may suspend or terminate your service if you breach this Policy. Depending on the severity, this may occur:

- With prior warning if the issue can be rectified; or
- Immediately and without notice if the breach is serious, unlawful, or requires urgent action.
- We may also be required by law or regulatory direction to suspend or terminate services.

7. Monitoring and Enforcement

Foxus is not obliged to monitor user activity but reserves the right to do so. We may:

- Remove or block content transmitted over our network;
- Cooperate with law enforcement or regulatory bodies in investigating violations;
- Take action (including suspension) to protect the integrity of our services.

8. Website and Content Blocking

Foxus may restrict or block access to websites or content if required by law, regulatory order, or if necessary to protect our network.

9. Amendments

Foxus may update this Policy at any time. Changes will be published on our website, and continued use of our services will constitute acceptance of the updated Policy.

Contact Us

For questions or concerns about this Policy:

Phone: 1800 036 987 (Mon–Fri, 9am–7pm AET; Sat–Sun, Closed)

Email: support@foxus.com.au

Mail: Foxus, PO Box 157, Broadway NSW 2007