

ACCEPTABLE USE POLICY

Effective Date: 5 August 2026

This Acceptable Use Policy ("Policy") governs the use of all websites, online services, software, digital products, e-learning platforms, customer portals, mobile applications and other services ("Services") provided by:

SafetyNet Americas Ltd

Company Number: **17366592**

20 Wenlock Road

London N1 7GU

England

By accessing or using any SafetyNet Service, you agree to comply with this Policy.

1. Purpose

The purpose of this Policy is to ensure the secure, lawful and responsible use of SafetyNet Services while protecting our customers, intellectual property, infrastructure and business operations.

This Policy applies to every visitor, customer, learner, subscriber, business partner and authorised user.

2. Compliance with Laws

Users shall comply with all applicable laws and regulations when using SafetyNet Services.

Users remain solely responsible for ensuring that their activities comply with local, national and international legislation applicable in their jurisdiction.

3. Lawful Use

Users may only use SafetyNet Services for lawful business, educational or personal purposes consistent with these Terms.

Services may not be used for any illegal, fraudulent or abusive activity.

4. Account Security

Users are responsible for maintaining the confidentiality of:

- usernames;
- passwords;
- authentication codes;
- account credentials.

Users shall immediately notify SafetyNet of any suspected unauthorised access.

Accounts may not be shared unless expressly authorised by SafetyNet.

5. Intellectual Property

All intellectual property remains the exclusive property of SafetyNet Americas Ltd or its licensors.

Except where expressly authorised, users shall not:

- copy;
- reproduce;
- distribute;
- publish;
- sublicense;
- modify;
- translate;
- sell;
- rent;
- lease;
- commercially exploit;
- create derivative works from any SafetyNet content.

6. Digital Products

Digital products are licensed for the authorised customer only.

Users shall not:

- upload products to file-sharing websites;
- distribute downloaded files;
- remove copyright notices;
- bypass licence restrictions;

- share download links;
- provide access to unauthorised persons.

7. E-learning Courses

Course access is personal unless a corporate licence expressly provides otherwise.

Users shall not:

- share login credentials;
- permit another person to complete a course in their name;
- falsify examination results;
- manipulate completion records;
- obtain certificates fraudulently.

SafetyNet may invalidate certificates obtained in breach of this Policy.

8. Software

Users shall not:

- reverse engineer software;
- decompile applications;
- disassemble executable files;
- circumvent technical protections;
- modify licence controls;
- interfere with software functionality.

9. Artificial Intelligence and Automated Systems

Without prior written permission, users shall not use SafetyNet content, software or Services to:

- train artificial intelligence models;
- develop machine learning datasets;
- create large language model training material;
- generate derivative AI products;
- harvest educational content for automated processing;
- create competing AI systems using SafetyNet materials.

10. Automated Access

Users shall not use:

- bots;
- web crawlers;
- spiders;
- scrapers;
- automated download tools;
- automated account creation;
- automated testing tools that place unreasonable load on the Services.

Reasonable indexing by recognised search engines is permitted where not otherwise restricted.

11. Security

Users shall not:

- attempt unauthorised access;
- bypass authentication systems;
- interfere with security controls;
- introduce malware;
- upload viruses;
- upload ransomware;
- distribute spyware;
- exploit vulnerabilities;
- conduct penetration testing without written authorisation;
- attempt denial-of-service attacks;
- interfere with network operations.

12. Data Collection

Users shall not collect personal information from the Website by automated or manual means except where expressly authorised by law.

Mass harvesting of email addresses, customer information or user data is prohibited.

13. False Information

Users shall not knowingly provide:

- false identity information;
- misleading registration details;
- fraudulent payment information;
- false certification information;
- inaccurate company details.

14. Unlawful Content

Users shall not upload, transmit or distribute content that is:

- unlawful;
- defamatory;
- threatening;
- abusive;
- discriminatory;
- obscene;
- fraudulent;
- infringing intellectual property rights;
- invasive of privacy;
- harmful to minors;
- intended to promote criminal activity.

15. Dangerous Activities

SafetyNet Services shall not be used to:

- facilitate unlawful handling of hazardous materials;
- evade legal compliance requirements;
- support criminal activity;
- circumvent export controls;
- bypass safety legislation;
- prepare fraudulent shipping documentation;
- generate false training certificates.

16. Third-Party Rights

Users shall respect the rights of third parties.

Users shall not upload content that infringes:

- copyright;
- trademarks;
- patents;
- trade secrets;
- confidential information;
- privacy rights.

17. Commercial Misuse

Users shall not:

- resell SafetyNet products without authorisation;
- operate unauthorised training businesses using SafetyNet materials;
- reproduce courses for commercial purposes;
- advertise competing products using SafetyNet Services.

18. Fair Use

Users shall not engage in activities that place unreasonable demands on SafetyNet infrastructure, including excessive downloading, excessive API requests or repetitive automated access that degrades system performance.

19. Monitoring

To protect our Services, SafetyNet may monitor system usage, investigate suspected misuse and review technical logs where reasonably necessary for security, fraud prevention or legal compliance, in accordance with applicable privacy laws.

20. Suspension and Termination

SafetyNet may suspend or terminate access, with or without prior notice, where it reasonably believes that a user has:

- violated this Policy;
- violated applicable law;

- infringed intellectual property rights;
- compromised system security;
- attempted fraud;
- misused training or certification services.

Suspension does not affect any other legal rights or remedies available to SafetyNet.

21. Reporting Abuse

Users who become aware of misuse or security concerns are encouraged to report the matter using the contact details published on the Website.

22. Limitation of Liability

SafetyNet shall not be liable for losses arising from suspension or termination of Services where such action is taken in accordance with this Policy or where reasonably necessary to protect our systems, users or legal interests, except to the extent liability cannot be excluded under applicable law.

23. Changes to this Policy

SafetyNet may amend this Policy from time to time.

The revised version will become effective upon publication on the Website unless otherwise stated.

Continued use of the Services after publication constitutes acceptance of the revised Policy.

24. Governing Law

This Policy shall be governed by and construed in accordance with the laws of England and Wales.

25. Jurisdiction

Subject to any mandatory consumer protection laws applicable in the user's country of residence, any dispute arising under or in connection with this Policy shall be subject to the exclusive jurisdiction of the courts of England and Wales.

26. Contact

Questions regarding this Acceptable Use Policy may be submitted using the contact information published on the SafetyNet website.

Copyright © 2026 SafetyNet Americas Ltd. All Rights Reserved.