Stirdie Acceptable Use Policy

Last modified on 19th April 2024

Our Commitment

Stirdie is committed to providing secure and trusted messaging solutions, through our systems, technology, people, and processes, we work tirelessly to provide solutions users can trust through data integrity, security and verification. . This policy is set to provide clear guidelines for users in their acceptable use of our services.

Our Policy

This policy applies to all users of Stirdie services. This policy does not replace nor cover all prohibited activities as covered by Stirdie Terms & Conditions.

When agreeing to the Terms and Conditions set out to use Stirdie services you agree to this Policy. The Services made available by Stirdie are to be used for permission-based and legitimate messaging purposes only. Stirdie services cannot be used for the following purposes:

- Messaging/advertising that fails to comply with relevant legislation
- Sending commercial electric messages without consent and valid opt-out
- Sending messages to recipients who have unsubscribed
- Sending messages that attempt to falsify an identify or misrepresent a brand
- Sending messages with fraudulent information or phishing attempts.
- Sending or receiving messages that contain unlawful or harmful content, including but not limited to content that contains:
    - non-consensual intimate images
    - sexual or pornographic material
    - child sexual exploitation material
    - extreme crime and violent material
    - pro-terror material
    - promotes counterfeit goods
    - abusive, harassing, bullying, intimidation, racial discrimination, hate group paraphernalia, murder, self-harm,
      extortion or blackmail
    - cruelty to animals or the sale or trade of endangered species
    - dangerous products or services, e.g. firearms (including fireworks)
    - alcohol, tobacco, or illegal drug material
    - gambling

Stirdie may implement measures to monitor account usage to identify spam or potential

fraudulent use of services through messages and/or misrepresentation of identity. In accordance with our Terms and Conditions, Stirdie may suspend access to Services without any notice where we identify services may be used or intended for use for unlawful purposes.
Users are responsible for ensuring that all messages sent using Stirdie comply with relevant local laws as well as relevant laws of the message destination country. Failure to comply with legal requirements may result in a delay or failure of message delivery. Messages classified as spam or that are in breach of governing legislation may be subject to financial and/or legal consequences.

Stirdie may provide services and features to support users in their compliance obligations, however, the Customer is responsible for ensuring compliance measures are implemented and messages are monitored to meet the needs of relevant regulatory requirements.

Regulatory Requirements

In addition to our Acceptable Use of Service Policy, Stirdie Users must ensure compliance with the following legislation, regulations, and best practice guidelines:

United States of America:

- Telephone Consumer Protection Act (TCPA)
- CAN-SPAM Act CTIA Messaging Principles & Best Practices
- American Data Privacy and Protection Act 2022
- California Consumer Privacy Act (CCPA)Utah Consumer Privacy Act 2023

Australia:

- Spam Act 2003
- C661:2022 Reducing Scam Calls and Scam SMS
- Privacy Act 1988
- Online Safety Act 2021

New Zealand:

- Unsolicited Electronic Messages Act 2007
- Compliant Electronic Marketing: Guidance for New Zealand Businesses
- Harmful Digital Communications Act 2015

For any questions or assistance, you can contact us at support@stirdie.com

Reporting

Users can report a breach of this policy and a complaint can be lodged by contacting

compliance@stirdie.com