Acceptable Use Policy for Quickport CRM

Effective Date: October 23, 2025
Last Updated: October 23, 2025

1. Introduction and Purpose

This Acceptable Use Policy ("AUP" or "Policy") defines the acceptable and prohibited uses of Quickport CRM services ("Service"), including our website (https://quickport.co.in), web application, APIs, mobile applications, and all related features.

Purpose:

- Protect the security, integrity, and availability of the Service for all users
- Ensure compliance with Indian laws and regulations (IT Act 2000, DPDPA 2023, TRAI regulations)
- Prevent abuse, spam, fraud, and other harmful activities
- Maintain the reputation and trustworthiness of the Quickport CRM platform
- Clarify user responsibilities and consequences for violations

This Policy is incorporated into and forms part of our Terms of Service. By using Quickport CRM, you agree to comply with this AUP. Violations may result in account suspension, termination, or legal action.

2. Scope and Applicability

This Policy applies to:

Who:

- All Quickport CRM subscribers (Foundation, Engage, Automate, Intelligence, Innovation tiers)
- Trial and free-tier users
- Account administrators, team members, and authorized users
- Anyone accessing Quickport CRM services or APIs

What:

- All features and services provided by Quickport CRM (messaging, customer management, campaigns, support tickets, analytics, APIs)
- Content you upload, create, transmit, or store through the Service (customer data, message templates, files, etc.)
- Use of third-party integrations (MSG91, Razorpay, ViaSocket, etc.) through Quickport CRM

3. Acceptable Use

You may use Quickport CRM for **lawful business purposes** consistent with our Terms of Service, including:

3.1 Permitted Activities

- **Customer Relationship Management**: Storing and managing customer profiles, contact information, interaction history, and sales data
- **Transactional Communications**: Sending OTPs, appointment reminders, order confirmations, payment receipts, and delivery updates to customers who have an existing relationship with your business
- **Consent-Based Marketing**: Sending promotional campaigns to customers who have explicitly opted in to receive such communications
- **Support Operations**: Managing support tickets, tracking customer issues, and providing customer service
- **Analytics**: Generating reports and insights from your customer data
- **Team Collaboration**: Sharing customer information with authorized team members for business purposes
- **API Integration**: Connecting Quickport CRM with other business tools via our APIs (within rate limits)
- **Compliance Management**: Maintaining records for DLT, DPDPA, and other regulatory requirements

3.2 Fair Use Guidelines

- Use the Service in accordance with your subscription tier limits (storage, users, messages, API calls)
- Respect rate limits and throughput caps (10-50 TPS depending on tier)
- Store only business-relevant data (not personal backups, media libraries, or non-CRM content)
- Use reasonable judgment when sending bulk communications

4. Prohibited Activities

The following activities are **strictly prohibited** when using Quickport CRM:

4.1 Illegal Activities

You must **NOT** use Quickport CRM to:

- Violate any applicable local, state, national, or international law, regulation, or order
- Engage in or facilitate illegal activities (fraud, money laundering, drug trafficking, human trafficking, etc.)
- Infringe intellectual property rights (copyright, trademark, patent, trade secret) of any third party
- Distribute child sexual abuse material (CSAM) or any illegal pornography
- Engage in illegal gambling or online betting operations
- Violate export control laws or economic sanctions

4.2 Spam and Unsolicited Communications

You must **NOT** use Quickport CRM to:

- Send unsolicited commercial messages (spam) to individuals who have not opted in
- Violate India's DLT (Distributed Ledger Technology) regulations or TRAI's TCCCPR 2018
- Use non-approved DLT templates, headers, or sender IDs
- Send promotional messages to DND (Do Not Disturb) registered numbers without explicit consent
- Harvest, scrape, or collect email addresses or phone numbers from third-party sources without authorization
- Send messages that misrepresent your identity, business, or affiliation
- Engage in "message bombing" (sending excessive messages to a single recipient to harass or overwhelm)
- Fail to honor opt-out requests within 24 hours

4.3 Abusive and Harmful Content

You must **NOT** use Quickport CRM to transmit, upload, or store:

- Threatening, abusive, defamatory, libelous, or harassing content
- Hate speech based on race, ethnicity, religion, caste, gender, sexual orientation, disability, or national origin

- Content that promotes violence, terrorism, or harm to individuals or groups
- Pornographic, sexually explicit, or obscene material (except in limited cases where legally permitted for business purposes, such as healthcare providers)
- Content that glorifies suicide, self-harm, or eating disorders
- Deceptive or fraudulent content (phishing messages, fake invoices, impersonation)

4.4 Security and System Integrity

You must **NOT**:

- Attempt to gain unauthorized access to Quickport CRM systems, servers, networks, or other users' accounts
- Probe, scan, or test the vulnerability of our systems or networks
- Bypass, disable, or interfere with security features, authentication mechanisms, or rate limits
- Introduce viruses, malware, ransomware, trojans, worms, or other malicious code
- Launch denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Use automated tools (bots, scrapers, spiders) to access the Service without authorization
- Reverse engineer, decompile, or disassemble any part of the Quickport CRM platform
- Share your account credentials with unauthorized third parties or create accounts on behalf of others without permission

4.5 Data Privacy Violations

You must **NOT**:

- Collect, store, or process personal data in violation of India's Digital Personal Data Protection Act, 2023 (DPDPA)
- Fail to obtain proper consent before processing personal data of customers or end-users
- Share customer data with third parties without authorization or legal basis
- Store sensitive personal data (SPDI) such as financial information, health records, or biometric data without adequate security measures
- Violate data retention policies (keeping data longer than necessary or required)
- Refuse to honor Data Principal rights (access, correction, erasure requests)

4.6 Misuse of Service Features

You must **NOT**:

- Resell, redistribute, or sublicense Quickport CRM services without written authorization
- Use Quickport CRM to provide services to your customers in a manner that competes with our business model
- Create multiple accounts to circumvent subscription tier limits or pricing
- Artificially inflate metrics (fake customer profiles, sham campaigns) to misrepresent usage or performance
- Use the Service to store or transmit content unrelated to CRM functions (personal file storage, media hosting, cryptocurrency mining scripts)
- Exceed API rate limits by creating multiple API keys or using undocumented endpoints[4][6][1][5]

4.7 Intellectual Property Violations

You must **NOT**:

- Use Quickport CRM to distribute pirated software, movies, music, or other copyrighted content without authorization
- Remove, alter, or obscure any proprietary notices, trademarks, or branding from Quickport CRM
- Use our trademarks, logos, or brand assets without prior written permission
- Copy, modify, or create derivative works of our platform, code, or documentation

4.8 Financial and Payment Abuse

You must **NOT**:

- Use stolen or fraudulent payment methods (credit cards, bank accounts, UPI IDs)
- Initiate chargebacks without first attempting to resolve billing disputes with us
- Manipulate billing systems to avoid paying for services used
- Use Quickport CRM to facilitate fraudulent transactions (fake invoices, payment scams, pyramid schemes)

5. Specific Compliance Requirements

5.1 DLT and TRAI Compliance (India)

You must:

- Register as a Principal Entity (PE) on a DLT platform before sending SMS or WhatsApp messages
- Use only DLT-approved templates, headers, and sender IDs
- Obtain and maintain records of customer consent for promotional messages
- Honor opt-out requests immediately (within 24 hours)
- Comply with message category rules (Service-Implicit, Transactional, Promotional)
- Whitelist all CTAs (links, phone numbers) before including them in messages

See our DLT Compliance Policy for full requirements.

5.2 DPDPA 2023 Compliance (India)

You must:

- Obtain free, specific, informed, unconditional, and unambiguous consent before collecting personal data
- Provide Data Principals with clear privacy notices
- Honor Data Principal rights (access, correction, erasure, nomination) within 30 days
- Store personal data securely and delete it when no longer needed
- Report data breaches to affected individuals and authorities as required

See our Privacy Policy for full requirements.

5.3 Anti-Spam and Anti-Phishing

You must:

- Clearly identify yourself as the sender of all messages
- Include accurate "From" information (business name, contact details)
- Provide a working opt-out mechanism in all promotional messages
- Never misrepresent message content or purpose
- Never impersonate government agencies, banks, or trusted brands

6. Enforcement and Consequences

6.1 Violation Detection

Quickport CRM uses a combination of methods to detect AUP violations:

- **Automated monitoring**: Pre-send validation of DLT templates, rate limit tracking, spam detection algorithms
- **User reports**: Abuse reports from recipients or other users (abuse@quickport.co.in)
- **Manual review**: Periodic audits of high-volume accounts or flagged content
- **Third-party alerts**: Notifications from MSG91, telecom operators, or law enforcement

6.2 Response to Violations

When we detect or are notified of an AUP violation, we may take the following actions:

Level 1: Warning (First-time minor violation)

- Email notification explaining the violation
- Guidance on how to correct the issue
- 7-day grace period to comply
- No service disruption if corrected within grace period[4]

Level 2: Suspension (Repeat or moderate violation)

- Temporary suspension of messaging features (SMS, WhatsApp, Email)
- Account access restricted to view-only mode
- Duration: 7-30 days depending on severity
- Reactivation requires written acknowledgment of violation and corrective action plan[4]

Level 3: Termination (Severe or persistent violation)

- Immediate account termination without refund
- Permanent ban from creating new accounts
- Data retained for 30 days for investigation, then deleted

- May involve notification to law enforcement for illegal activities

6.3 Examples of Violation Severity

Minor (Warning):

- Using an unapproved DLT template once
- Exceeding rate limits due to configuration error
- Failing to update consent records promptly

Moderate (Suspension):

- Sending promotional messages to DND numbers repeatedly
- Ignoring multiple opt-out requests
- Storing excessive non-business data

Severe (Termination):

- Sending spam to thousands of recipients
- Distributing illegal content (CSAM, pirated software)
- Hacking attempts or security breaches
- Using stolen payment methods
- Repeated violations after warnings

6.4 Appeals Process

If you believe your account was suspended or terminated in error:

1. Email **crm@quickport.co.in** with subject "AUP Appeal - [Account ID]"
2. Provide evidence supporting your appeal (logs, consent records, DLT approvals)
3. We will review within **7 business days** and respond with a decision
4. If the appeal is denied, you may escalate to our Grievance Officer (Jidnyasa Gunjal, +91 9422228848) for final review within **30 days**

7. Reporting Abuse

7.1 How to Report Violations

If you become aware of AUP violations by another Quickport CRM user:

Email: crm@quickport.co.in
Subject: "AUP Violation Report - [Brief Description]"

Include:

- Description of the violation
- Evidence (screenshots, message headers, phone numbers, URLs)
- Your contact information
- Date and time of the incident

Response Time: We will acknowledge reports within **24 hours** and investigate within **5 business days**.[5][1][4]

7.2 Confidentiality

Reports are handled confidentially. We do not disclose the identity of reporters unless required by law or necessary to resolve the issue.

7.3 Protection Against Retaliation

Quickport CRM prohibits retaliation against users who report AUP violations in good faith. If you experience retaliation, report it immediately to crm@quickport.co.in.

8. User Responsibilities

8.1 Account Security

You are responsible for:

- Keeping your login credentials (email, password, JWT tokens) confidential
- Enabling Multi-Factor Authentication (MFA) where available
- Logging out of shared or public devices
- Notifying us immediately of unauthorized access (crm@quickport.co.in)

8.2 Content Monitoring

You are responsible for:

- Monitoring content uploaded or transmitted by team members with access to your account
- Ensuring all content complies with this AUP
- Promptly removing violating content when notified

8.3 Third-Party Compliance

If you grant access to third-party applications or services (via API keys or integrations):

- You remain responsible for all activities conducted through those integrations
- Ensure third parties comply with this AUP
- Revoke access immediately if violations occur

9. Limitation of Liability

While Quickport CRM takes reasonable measures to enforce this AUP, we are not responsible for:

- Violations committed by users
- Damages caused by user-generated content
- Third-party claims arising from your use of the Service
- Losses resulting from account suspension or termination due to AUP violations

You agree to indemnify and hold harmless Quickport CRM from any claims, liabilities, or damages arising from your violation of this AUP (see Terms of Service, Section 12 for full indemnification terms).

10. Cooperation with Law Enforcement

Quickport CRM cooperates with law enforcement agencies and regulatory authorities when required:

- We may disclose user information in response to valid legal requests (court orders, subpoenas)
- We report illegal activities (child exploitation, terrorism, fraud) to appropriate authorities
- We preserve evidence and logs as required by law (CERT-In, TRAI, Data Protection Board)

Users are notified of law enforcement requests when legally permitted.

11. Changes to This Policy

We may update this Acceptable Use Policy to reflect:

- Changes in laws or regulations (DPDPA, TRAI, IT Act)
- New features or services
- Evolving security threats or abuse patterns

Notification Method:

- Email to registered users **30 days before** material changes take effect
- In-app notification upon login
- Updated "Last Updated" date at the top of this document

Your continued use of Quickport CRM after updates constitutes acceptance of the revised AUP.

12. Contact Information

For questions, clarifications, or to report AUP violations:

Quickport CRM
General Inquiries: crm@quickport.co.in
Abuse Reports: crm@quickport.co.in
Grievance Officer: Jidnyasa Gunjal
Mobile: +91 9422228848
Website: https://quickport.co.in
UDYAM Registration: MH180408716

Business Hours: Monday - Friday, 9:00 AM - 6:00 PM IST
Response Time: 24-48 hours for AUP inquiries; 24 hours for abuse reports

13. Acknowledgment and Agreement

By using Quickport CRM, you acknowledge that:

- You have read and understood this Acceptable Use Policy
- You agree to comply with all terms and conditions outlined above
- You understand that violations may result in account suspension, termination, or legal action
- This Policy is legally binding and incorporated into our Terms of Service

Failure to comply with this AUP may result in immediate termination of your account and legal consequences under Indian law (IT Act 2000, DPDPA 2023, IPC).

END OF ACCEPTABLE USE POLICY

Document Version: 1.0
Prepared by: Quickport CRM Legal & Compliance Team
Next Review Date: April 23, 2026
References: IT Act 2000, DPDPA 2023, TRAI TCCCPR 2018, Terms of Service