PP Capital
Your Profit. Our Aim.

PAWAN PARMESHWAR CAPITAL PVT LTD

Regd. Office: 187, Dadiseth Agyari Lane, 4th Floor, Singhania Wadi, Mumbai – 400 002
Head Office: 136-138, ORM Wing B Co-Op Premises Soc. Ltd., Ground Floor, Royal Palm, Goregaon East, Mumbai – 400 065
Tel: 022-22014936 / 4961 3718

Member: NSE Code: 00188 | BSE Code: 0550

MOBILE PHONE USAGE POLICY

(Use of Mobile Phones, Messaging Applications and Personal Communication Devices)

Document Control

Policy Name	Mobile Phone Usage Policy
Version	1.0
Effective Date	16-10-2025
Approved By	Board of Directors, Pawan Parmeshwar Capital Pvt Ltd
Owner	Compliance Officer (Mr. Rajkumar Pandey)
Review Frequency	Annual or upon material regulatory change
Supersedes	Nil — new policy issued in November 2025

1. Preamble and Objective

Pawan Parmeshwar Capital Pvt Ltd (the "Company") is a Trading Member of NSE and BSE and a SEBI-registered stock broker. This Mobile Phone Usage Policy (the "Policy") establishes the rules for use of mobile phones, smart phones, tablets, messaging applications and other personal communication devices by all Covered Persons of the Company in connection with the Company's business.

The Policy is essential to the Company's compliance with multiple SEBI regulatory requirements concerning: (i) recording of client orders received through telephonic channels; (ii) prevention of circulation of unauthenticated news; (iii) confidentiality of Unpublished Price Sensitive Information (UPSI); (iv) prevention of front-running; (v) cyber security and protection of confidential client data; and (vi) maintenance of an auditable trail of all client communications.

The Policy is intended to:

- Prevent the use of mobile phones and messaging applications as a channel for receiving client orders, circulating unverified market information, or communicating UPSI;

- Ensure that all client orders received over the telephone are received on the Company's recorded lines, in accordance with SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/108 dated September 26, 2017;
- Implement appropriate internal controls under Regulation 9A of the SEBI (Prohibition of Insider Trading) Regulations, 2015 to prevent leak of UPSI through mobile devices;
- Implement the access-control restriction under SEBI Circular Cir/ISD/1/2011 dated March 23, 2011 in relation to chat forums, messenger sites and the like; and
- Implement appropriate cyber security controls in respect of mobile devices that have access to the Company's information systems, in accordance with the SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024.

2. Scope and Applicability

This Policy applies to all Covered Persons of the Company in respect of:

- Use of any mobile phone, smart phone, tablet or similar mobile communication device (whether Company-issued or personally owned) in or about the Company's office premises and dealing room;
- Use of any mobile phone or other communication device for communication with the Company's clients, counterparties, listed-company contacts or other third parties in respect of the Company's business;
- Use of messaging applications (including, without limitation, WhatsApp, Telegram, Signal, Microsoft Teams, Slack, iMessage, Google Messages, Snapchat, Discord and similar applications) in any matter relating to the Company's business; and
- Use of social media applications and chat forums in any matter relating to the Company's business.

Although the Company is currently engaged primarily in institutional broking, this Policy applies as a comprehensive compliance framework regardless of the categories of clients serviced from time to time.

3. Regulatory References

This Policy is framed in accordance with the following Indian regulations and circulars, as amended from time to time:

3.1 Recording of Client Orders

- SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/108 dated September 26, 2017 — Prevention of Unauthorised Trading by Stock Brokers, mandating that where order instructions are received from clients through the telephone, the stock broker shall mandatorily use a telephone recording system to record the instructions and maintain telephone recordings as part of its records;

- SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/124 dated November 30, 2017 — Clarifications on the requirement to record client instructions;
- SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2018/109 dated January 11, 2018 — Further clarifications, effective from April 1, 2018;
- SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025 — consolidating the above requirements.

3.2 Prevention of Circulation of Unauthenticated News

- SEBI Circular Cir/ISD/1/2011 dated March 23, 2011 — Unauthenticated news circulated by SEBI Registered Market Intermediaries through various modes of communication (incorporated in Paragraph 2.3 of the SEBI Master Circular on Surveillance of Securities Market dated September 23, 2024);
- SEBI Master Circular on Surveillance of Securities Market SEBI/HO/ISD/ISD-PoD-2/P/CIR/2024/126 dated September 23, 2024 — in particular Paragraph 2.3 (Internal Code of Conduct of SEBI Registered Market Intermediaries to prevent circulation of unauthenticated news).

3.3 Insider Trading and UPSI

- SEBI (Prohibition of Insider Trading) Regulations, 2015 (as last amended on March 11, 2025) — Regulation 3 (prohibition on communication of UPSI), Regulation 4 (prohibition on trading while in possession of UPSI), and Regulation 9A (internal control systems including UPSI confidentiality).

3.4 Fraudulent and Unfair Trade Practices

- SEBI (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003 (as last amended on June 28, 2024) — Regulation 4(2)(q) (front-running by intermediaries).

3.5 Cyber Security

- SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 — Cyber Security and Cyber Resilience Framework for Stock Brokers / Depository Participants;
- SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2024/113 dated August 20, 2024 — Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities, including baseline security requirements for mobile applications under the Identity Management, Authentication and Access Control control family;

- SEBI Circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2025/60 dated April 30, 2025 — Clarifications to the CSCRF.

3.6 Other

- SEBI (Stock Brokers) Regulations, 1992 — Schedule II Code of Conduct for Stock Brokers.

4. Definitions

"Covered Persons": All Directors, the Compliance Officer, the Principal Officer (PMLA), Key Managerial Personnel, dealers, research team members, sales personnel, operations and back-office staff, IT personnel, authorised persons and all other employees, consultants and other persons performing functions on behalf of the Company.

"Company-Issued Device": Any mobile phone, smart phone, tablet or similar mobile communication device issued to a Covered Person by the Company for performance of duties.

"Dealing Room": The area of the Company's office where dealers, traders, the institutional sales / dealing desk and other personnel involved in order execution work, and where the Company's recorded telephone lines and order management systems are operated.

"Messaging Application": Any messaging or chat application, including but not limited to WhatsApp, Telegram, Signal, Microsoft Teams, Slack, iMessage, Google Messages, Snapchat, Discord, and any other application that permits exchange of text, audio, video, image or file messages between users.

"Personal Device": Any mobile phone, smart phone, tablet or similar mobile communication device personally owned by a Covered Person.

"Recorded Line": A telephone line of the Company on which incoming and outgoing calls are recorded by the Company's telephone recording system, and the recordings of which are preserved by the Company in accordance with the SEBI requirements set out in Section 3.1.

"UPSI": Unpublished Price Sensitive Information as defined in Regulation 2(1)(n) of the SEBI (Prohibition of Insider Trading) Regulations, 2015.

5. Use of Mobile Phones in the Dealing Room

5.1 General Restriction

To ensure that all client orders are received only through the Company's Recorded Lines or other approved electronic channels, and that there is a complete and reliable audit trail of all client communications, the following restrictions apply in the Dealing Room:

- Personal Devices shall not be used by any dealer or other Dealing Room personnel for receiving any client order, instruction, modification, cancellation or confirmation;
- Personal Devices shall not be used to communicate any UPSI or any client-specific information of a confidential nature;
- Personal Devices shall not be used to take any photograph, screen capture, screen recording or video of any trading terminal, screen, document or other Company property in the Dealing Room;
- Personal Devices shall be kept on silent or vibrate mode and shall not be used during active dealing hours except for brief, non-client communications.

5.2 Company-Issued Devices

Where the Company issues a Company-Issued Device to a Covered Person, the following terms apply:

- The device shall be used solely for the purposes of the Company's business;
- All calls on the Company-Issued Device with clients shall be made and received in such a manner as to ensure that the conversation is recorded on the Company's telephone recording system, in accordance with SEBI Circular dated September 26, 2017;
- The device shall be configured by the Company's IT function to require password / biometric authentication, screen lock and remote wipe in the event of loss or theft;
- The Compliance Officer shall maintain a register of all Company-Issued Devices, the Covered Persons to whom they are issued, and the dates of issue and return.

6. Client Communications by Telephone and Mobile

6.1 Receipt of Client Orders

In accordance with SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/108 dated September 26, 2017, the Company shall execute trades on behalf of any client only after keeping evidence of the client placing the order. Permitted channels for receipt of client orders are:

- Orders received in writing from the client, signed by the client or an authorised signatory of the client;
- Orders received from the client's authorised email address (with verification by the Dealing Room before execution);
- Orders received over the Company's Recorded Lines;
- Orders received through the Company's approved electronic order entry platform (BITS or equivalent).

Orders shall not be accepted or acted upon if received through any of the following channels:

- Voice call on any Personal Device;
- WhatsApp, Telegram, Signal or any other Messaging Application;
- Social media platform (including direct messages on LinkedIn, X, Facebook, Instagram or similar);
- SMS / text message on any device, except where the SMS is from an authorised source and has been confirmed in writing by the client;
- Verbal instructions communicated in person or over an unrecorded line.

6.2 Exceptional Circumstances — Travel and Off-Site

Where a dealer or other authorised Covered Person is, with the prior written approval of the Compliance Officer, required to be off-site (such as on business travel, at a client meeting or while attending an industry event) and is required to take a client order outside the office, the following process shall be followed:

- Prior written approval of the Compliance Officer shall be obtained, in the format at Annexure B, recording the dates, location, the clients in respect of whom the off-site arrangement applies, and the specific reason;
- The Covered Person shall, immediately on receipt of any order off-site, contact the Dealing Room over a Recorded Line and re-state the order on that line, so as to create the recorded audit trail required by SEBI;
- The Covered Person shall not, in any case, execute the order directly from the Personal Device;
- The Covered Person shall maintain a written record of the off-site order receipt and shall hand it over to the Compliance Officer on return to office.

6.3 Recording of Calls

All Recorded Lines shall be configured to record both incoming and outgoing calls. Recordings shall be preserved for a minimum period of three years (being the period for which SEBI accepts investor complaints), in accordance with SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/124 dated November 30, 2017. Where any client dispute has been raised, recordings shall be preserved until final resolution of the dispute. Where SEBI directs that specific records be preserved, the Company shall preserve them until further intimation by SEBI.

7. UPSI Communication over Mobile Phones and Messaging Applications

Unpublished Price Sensitive Information is, by its nature, required to be handled on a strict need-to-know basis. To support compliance with Regulation 3 of the SEBI (Prohibition of Insider Trading) Regulations, 2015 and the Company's Insider Trading Code (Version 2.0):

7.1 Prohibition on UPSI over Mobile

- UPSI shall not be communicated by any Covered Person to any other person over any Personal Device, Messaging Application or social media platform, regardless of whether the recipient is internal or external;
- UPSI may be communicated only over the Company's recorded telephone lines, the Company's email system or through such other auditable, recorded channels as the Compliance Officer may approve;
- Where UPSI is communicated, the requirements of Section 6 of the Insider Trading Code (Need-to-Know Principle, Confidentiality Agreements, Wall Crossing) and Section 7 of that Code (Structured Digital Database) shall be observed.

7.2 Prohibition on Front-Running Channels

Per Regulation 4(2)(q) of the SEBI (PFUTP) Regulations, 2003, front-running by an intermediary in relation to client trades is prohibited. To prevent any channel of front-running through mobile-based communications:

- No Covered Person shall, by any Personal Device, Messaging Application or other unofficial channel, communicate any pending or contemplated client order, the identity of the client, the price or quantity, or any other details of any pending client order to any third party;
- No Covered Person shall trade, or cause any other person to trade, in advance of a pending client order, on the basis of knowledge of that order.

8. Circulation of Market News, Rumours and Unauthenticated Information

Per SEBI Circular Cir/ISD/1/2011 dated March 23, 2011 (incorporated into Paragraph 2.3 of the SEBI Master Circular on Surveillance dated September 23, 2024) and the Company's adopted Policy for Unauthentic News Circulation:

8.1 Prohibition on Circulation of Unauthenticated News

- Covered Persons (including Directors, Officers, Employees, Temporary Staff and Voluntary Workers) shall not circulate any unauthenticated news related to any scrip in any blog, chat forum, email, SMS, Messaging Application or by any other mode of communication;

- Covered Persons shall not encourage or circulate rumours or unverified information obtained from any client, industry source, trade source or other source, without verification;
- Any market-related news received by a Covered Person in any official email, personal email, blog, SMS or message (including on a Messaging Application) shall be forwarded only after it has been seen and approved by the Compliance Officer.

8.2 Access Control to Chat Forums and Messenger Sites

Per Paragraph 2.3 of the SEBI Master Circular on Surveillance dated September 23, 2024:

- Access to chat forums and messenger sites on the Company's office systems shall be restricted; only senior officials authorised by the Board (which shall include the Compliance Officer) shall have access;
- All logs of such sites shall be treated as records of the Company and shall be maintained by the Compliance Officer;
- The Company shall implement appropriate technical controls to prevent unauthorised access to such sites from office systems.

8.3 Failure to Comply

Per Paragraph 2.3.5 of the SEBI Master Circular on Surveillance dated September 23, 2024, an employee who fails to forward market-related news only after Compliance Officer approval shall be deemed to have violated the provisions of the SEBI Act, the rules and regulations framed thereunder, and shall be liable to action. The Compliance Officer shall also be held liable for breach of duty in this regard.

9. Use of Messaging Applications and Social Media

9.1 Prohibition on Use for Business

- Messaging Applications shall not be used to receive or transmit any client order, instruction, modification, cancellation or confirmation;
- Messaging Applications shall not be used to communicate any UPSI;
- Messaging Applications shall not be used to communicate any confidential client information (including but not limited to client identity, client account details, client positions, client orders or client trading strategies);
- Messaging Applications shall not be used to share any internal Company information of a sensitive or confidential nature.

9.2 Limited Permitted Use

Messaging Applications may be used by Covered Persons for the following limited purposes, subject to the prohibitions in Section 9.1:

- Coordination of meetings, logistics and other administrative matters that do not involve disclosure of client information or UPSI;
- Internal team coordination on non-confidential operational matters.

9.3 Social Media

- No Covered Person shall publish, post, like, share or comment on any social media platform (including but not limited to LinkedIn, X, Facebook, Instagram, YouTube, Reddit) in respect of any specific scrip, client, trade or transaction of the Company, or any UPSI, or any unauthenticated news / rumour, without the prior written approval of the Compliance Officer;
- Posts of a personal nature on personal social media accounts that do not relate to the Company's business are permitted; however, Covered Persons should be mindful that their conduct on personal social media should not bring the Company into disrepute.

10. Cyber Security Requirements for Mobile Devices

In accordance with the SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024 (as clarified on April 30, 2025), the following controls apply to all mobile devices that have access to the Company's information systems, email or business data:

10.1 Authentication and Access Control

- Every Company-Issued Device shall be protected by a strong password or biometric authentication;
- Auto-lock shall be enabled with a screen-lock timeout of not more than five minutes;
- The Company shall be able to remotely lock or wipe a Company-Issued Device in the event of loss, theft or termination of the Covered Person's engagement.

10.2 Encryption and Storage

- Device-level encryption shall be enabled on every Company-Issued Device;
- Confidential client information shall not be stored on Personal Devices;
- Session login details for the Company's trading or back-office systems shall not be stored on any mobile device (in accordance with the SEBI Internet-Based Trading framework).

10.3 Permitted Applications

- Only applications approved by the Company's IT function shall be installed on Company-Issued Devices for accessing the Company's information systems;
- "Jail-broken" or "rooted" devices shall not be used to access the Company's information systems.

10.4 Loss, Theft and Decommissioning

- Loss or theft of any mobile device used for the Company's business (whether Company-Issued or Personal Device with business email installed) shall be reported to the Compliance Officer and the IT function within 24 hours;
- On termination or change of role, the Covered Person shall return any Company-Issued Device and shall co-operate with the Company in removing any business data from any Personal Device on which it has been stored or accessed.

11. Monitoring and Audit

- The Compliance Officer shall periodically review compliance with this Policy by all Covered Persons;
- The Compliance Officer may direct random or surprise checks in the Dealing Room to verify that Personal Devices are not being used for receiving client orders or for any prohibited purpose under this Policy;
- Compliance with this Policy shall form part of the scope of the half-yearly internal audit conducted under the SEBI framework for stock brokers;
- The Compliance Officer shall maintain a register of breaches of this Policy, the Covered Persons concerned, the action taken and the date of closure.

12. Sanctions for Non-Compliance

Non-compliance with this Policy may attract:

- Disciplinary action by the Company including warning, wage freeze, suspension, recovery or termination of engagement, in accordance with the Company's HR framework and (where applicable) Clause 10 of Schedule C of the SEBI (Prohibition of Insider Trading) Regulations, 2015;
- Reporting to the Stock Exchange and SEBI where the breach also constitutes a violation of any applicable SEBI Regulation or Circular (including, in case of breach of the Insider Trading Code, reporting in the standardised format prescribed by SEBI in Annexure 2 of the Master Circular on Surveillance dated September 23, 2024);
- Regulatory action by SEBI and / or the Stock Exchanges under the SEBI Act, 1992 and the relevant regulations; and

- In appropriate cases, criminal prosecution under applicable laws.

13. Cross-Policy References

This Policy shall be read together with the following adopted policies of the Company. Where any of these policies prescribes a more specific or more onerous requirement on a matter dealt with in this Policy, that requirement shall prevail.

- Conflicts of Interest Policy (Version 2.1) — for the broader conflicts framework;
- Insider Trading Code (Version 2.0) — for handling of UPSI, Structured Digital Database, Wall Crossing, Personal Account Dealing, Trading Window and Contra-Trade restrictions;
- Policy for Unauthentic News Circulation — for the prohibition on circulation of unauthenticated news under SEBI Circular Cir/ISD/1/2011 dated March 23, 2011;
- Order Acceptance Policy — for the broader framework on receipt of client orders through approved channels;
- Internal Control Policy — for the broader internal control framework;
- Anti-Money Laundering Policy — for restrictions on tipping off and on disclosure of STR / CTR filings under Section 12A of the Prevention of Money Laundering Act, 2002;
- Registers & Records Manual — for record-keeping and retention requirements relating to call recordings and other records.

14. Policy Review and Effective Date

- This Policy shall be reviewed at least once every financial year by the Compliance Officer and placed before the Board for re-approval;
- The Policy shall be reviewed earlier on the occurrence of any material amendment to: (a) SEBI's circulars on recording of client orders or on Unauthenticated News; (b) the SEBI (Prohibition of Insider Trading) Regulations, 2015; (c) the SEBI Cybersecurity and Cyber Resilience Framework; or (d) on any inspection / audit / regulatory observation requiring revision;
- This Policy shall come into effect from the date of its approval by the Board of Directors.

Annexure A — Acknowledgement and Undertaking by Covered Person

Every Covered Person shall sign this Acknowledgement at induction and on every annual refresher.

I, ____ (Name), holding the designation of ______________________________________ at Pawan Parmeshwar Capital Pvt Ltd, hereby acknowledge and undertake that:

- I have received a copy of the Mobile Phone Usage Policy (Version 1.0) of the Company, and I have read and understood its contents;
- I undertake to comply with the Policy in letter and spirit, including the restrictions on use of Personal Devices in the Dealing Room, the prohibition on receipt of client orders other than through the Company's approved channels, the prohibition on communication of UPSI over mobile and messaging applications, the prohibition on circulation of unauthenticated news, and the cyber security requirements for mobile devices;
- I undertake to forward any market-related news received by me in any official email, personal email, blog, SMS or message (including on any Messaging Application) only after it has been seen and approved by the Compliance Officer;
- I undertake to report any loss or theft of any mobile device used for the Company's business to the Compliance Officer and the IT function within 24 hours;
- I am aware that non-compliance with this Policy may attract disciplinary action by the Company, reporting to the Stock Exchanges and SEBI (where the breach also constitutes a regulatory violation), and regulatory or criminal proceedings under applicable laws.

Signature: _____________________________________ Date: ________________

Witnessed by Compliance Officer: _____________________________________

Annexure B — Approval for Off-Site Receipt of Client Orders

To be submitted to the Compliance Officer in advance, where a Covered Person is required to be off-site and to receive client orders in such circumstances.

Name of Covered Person	
Designation	
Period of off-site arrangement (Dates)	
Location(s)	
Specific reason / business purpose	
Name(s) of client(s) in respect of whom the arrangement applies	
Mobile number to be used during off-site period	
Confirmation of process	I confirm that I shall, immediately upon receipt of any order off-site, contact the Dealing Room over a Recorded Line and re-state the order on that line so as to create the recorded audit trail required by SEBI. I shall not execute the order directly from any Personal Device.
Signature & Date of Covered Person	
Compliance Officer decision (Approved / Rejected / Conditional)	
Conditions (if any)	
Signature & Date of Compliance Officer	

Annexure C — Register of Company-Issued Devices

To be maintained by the Compliance Officer (or designated IT custodian under the Compliance Officer's supervision).

S. No.	Name of Covered Person	Designation	Device Model / IMEI	Mobile Number	Date of Issue	Date of Return
1.						
2.						
3.						

Annexure D — Board Approval

This Mobile Phone Usage Policy (Version 1.0) has been reviewed and approved by the Board of Directors of Pawan Parmeshwar Capital Pvt Ltd at its meeting held on 16-10-2025.

The Board has also recorded, on the same date, the following:

- Compliance Officer for this Policy: Mr. Rajkumar Pandey;
- Frequency of review of this Policy: annual;
- List of senior officials authorised under Section 8.2 to access chat forums and messenger sites: ______________________________ (to be notified separately by Board minute).

For PAWAN PARMESHWAR CAPITAL PVT. LTD.

P K Choudhary

Director / Authorised Signatory

PAWAN PARMESHWAR CAPITAL PVT. LTD. MUMBAI

Director / Authorised Signatory

Name: Pawankumar Choudhary

Designation: Director

Date: 16-10-2025

Place: Mumbai