PRIVACY & DATA PROTECTION POLICY

OF

FLAT WHITE CAPITAL PRIVATE LIMITED

SUMMARY OF POLICY:

Policy Name	PRIVACY & DATA PROTECTION POLICY
Date of Approval of First Version	17-12-2025
Periodicity of Review	Annual
Prepared By	Prakhar Khandelwal
Approver	Board of Directors

Date of Review	Date of Next Review	Comments/Remarks/Changes
17-12-2025	On or before Dec-2026	Policy Approved

PRIVACY & DATA PROTECTION POLICY

1. Background

This Privacy & Data Protection Policy is framed in accordance with the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, applicable RBI directions, and other relevant laws. The policy governs the collection, use, storage, sharing, and protection of personal and sensitive personal data by FLAT WHITE CAPITAL PRIVATE LIMITED (FWCPL).

2. Purpose

The purpose of this Policy is to:

- Protect the privacy and confidentiality of customers, employees, vendors, and business partners
- Establish transparent practices for handling personal and sensitive personal data
- Ensure compliance with regulatory and statutory requirements
- Prevent unauthorized access, misuse, or disclosure of information

3. Definitions

FLAT WHITE CAPITAL PRIVATE LIMITED: Refers to FWCPL and its authorized representatives.
Personal Information: Any information that identifies or can reasonably identify an individual, directly or indirectly.
Sensitive Personal Data or Information: Includes financial information, passwords, biometric data, KYC documents, and other information as defined under applicable laws.
Data Subject: Any individual whose personal data is collected or processed by FWCPL.

4. Scope & Applicability

This Policy applies to:

- All customers, borrowers, employees, directors, contractors, vendors, and service providers
- All forms of data collection – physical, digital, telephonic, CCTV, and electronic
- All systems, applications, branches, and third-party platforms used by FWCPL

All employees and outsourced staff are required to comply with this Policy.

5. Collection of Information

FWCPL may collect personal information through online or offline modes for legitimate business purposes.

Key principles:

- Data shall be collected only with lawful basis such as consent, contractual necessity, or legal obligation
- Only minimum data required for the stated purpose shall be collected
- Optional data fields, if any, shall be clearly identified
- Data collection methods shall be transparent and fair

6. Use of Information

Personal information may be used for:

- Customer onboarding, KYC, and due diligence
- Loan appraisal, sanction, disbursement, servicing, and recovery
- Credit underwriting and portfolio monitoring
- Regulatory reporting and audit requirements
- Fraud prevention, risk management, and internal controls
- Grievance redressal and customer communication

7. Data Retention & Disposal

- Personal data shall be retained only for as long as required for business, legal, or regulatory purposes
- Retention periods shall be defined as per internal retention schedules
- Upon expiry of retention period, data shall be securely destroyed, anonymized, or de-identified
- Physical records shall be shredded; electronic records shall be permanently deleted

8. Sharing & Disclosure of Information

FWCPL shall not disclose personal information except:

- With explicit consent of the data subject
- To regulators, statutory authorities, or law enforcement agencies as required by law
- To approved third-party service providers under contractual confidentiality obligations

All third parties must adhere to equivalent data protection and confidentiality standards.

9. Information Security Controls

FWCPL shall implement reasonable security practices including:

- Role-based access controls and user authentication
- Secure servers and encrypted databases
- Physical security for branch records and vaults
- Regular system audits, vulnerability assessments, and access reviews
- Board-approved Business Continuity and Disaster Recovery arrangements

10. CCTV, Call Recording & Digital Data

- CCTV footage is used solely for security, audit, and compliance purposes
- Call recordings may be used for quality monitoring and dispute resolution
- Access to such data shall be restricted and monitored

11. Cookies & Website Data (If Applicable)

FWCPL websites or digital platforms may use cookies or similar technologies to:

- Improve user experience
- Analyse website usage
- Enhance security

Such data shall be treated as confidential and protected by appropriate safeguards.

12. Third-Party Links

FWCPL websites may contain links to external websites. FWCPL shall not be responsible for the privacy practices of such third-party sites, and users are encouraged to review their privacy policies separately.

14. Data Subject Rights

Data subjects may:

- Request access to their personal information
- Seek correction of inaccurate or outdated data
- Raise concerns regarding misuse or unauthorized disclosure

Requests shall be addressed in accordance with applicable laws and internal procedures.

15. Data Breach & Incident Management

- Any actual or suspected data breach must be immediately reported to the Compliance / IT team
- Incidents shall be investigated, documented, and remediated
- Regulatory reporting shall be done wherever required

16. Employee Responsibility & Training

- All employees and outsourced staff shall sign confidentiality undertakings
- Periodic training on data privacy and information security shall be conducted
- Any violation of this Policy may attract disciplinary action

17. Consent

By availing FWCPL services or interacting with its platforms, the data subject provides consent for collection, use, storage, and disclosure of information as per this Policy.