Jonathan Smith & Partners

SOLE PROPRIETOR: JONATHAN SMITH

FINANCIAL ADVISERS

MORTGAGE, FINANCE & PROTECTION INSURANCE:

Westbourne House, 1 Westbourne Crescent, SOUTHAMPTON, SO17 1EA.

Tel: 023 8058 4644 Mobile: 07717 772940

JONATHAN SMITH & PARTNERS

Data Protection Policy and Procedure

Version: 1

Policy Owner & Role:

INTERIM PERMISSIONS No. 001606
AUTHORISED AND REGULATED BY THE FINANCIAL CONDUCT AUTHORITY No. 125272
DATA PROTECTION REGISTRATION No. Z5420676
WEBSITE: WWW.MORTGAGE-NEXT.COM JRDSmith@Gmail.com

Version Control

Version Number:	Date:	Version Author:	Approval By:	Approval Date:	Revisions/ changes
1	01/07/2026	JONATHAN SMITH	JONATHAN SMITH	01/07/2026	NONE

1. **PURPOSE** is committed to protecting the privacy, confidentiality, integrity and availability of personal data. Jonathan Smith & Partners recognises that effective data protection is fundamental to maintaining customer trust, delivering good customer outcomes and meeting its legal and regulatory obligations.

Jonathan Smith & Partners shall process personal data in accordance with UK GDPR, the Data Protection Act 2018, PECR and all applicable FCA requirements.

The purpose of this policy is to establish a framework for the lawful, fair and transparent processing of personal data and to ensure that appropriate organisational and technical measures are implemented to protect personal information.

2. REVIEW OF POLICY

This policy will be reviewed regularly, at least once a year, and amended as considered necessary by Mr Jonathan Smith, Sole Trader, in the event of changing circumstances or regulations.

3. RESPONSIBILITIES

3.1 MANAGEMENT

My firm as a Sole Trader is made up of myself, Mr Jonathan Ronald David Smith, and is responsible for implementing this Data Protection Policy and ensuring it is followed

Responsibilities include:

Sole Trader
- Approving the policy
- Receiving regular management information
- Reviewing breaches and emerging risks

Jonathan Smith is the designated ICO Officer and Data Protection lead.

Responsibilities include:

- Monitoring compliance
- Maintaining records of processing activities
- Managing data breaches
- Overseeing DPIAs
- Liaising with regulators

3.2 EMPLOYEE

Employee's responsibilities include:

- Following this policy
- Completing mandatory training
- Reporting incidents immediately

4. DATA PROTECTION PRINCIPLES

Jonathan Smith & Partners shall ensure personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Protected through appropriate security measures
- Processed in a manner that demonstrates accountability

5. LAWFUL BASIS FOR PROCESSING

Jonathan Smith & Partners relies upon the following lawful bases:

- Contract
- Legal Obligation
- Legitimate Interests
- Consent (where appropriate)

Jonathan Smith & Partners maintains documented records evidencing the lawful basis relied upon for each processing activity.

6. SPECIAL CATEGORY DATA

Where Jonathan Smith & Partners processes information relating to health, vulnerability, ethnicity, religion or other Special Category Data, an Article 9 condition shall be identified and documented.

An Article 9 (Article 9: Substantial Public Interest (for safeguarding vulnerable customers and meeting FCA requirements) and/or Explicit Consent where appropriate) condition refers to the additional legal basis required under the UK GDPR (and GDPR) when processing Special Category Data.

Processing shall be limited to the minimum amount necessary.

7. PRIVACY NOTICES

Privacy Notices shall be provided at the point personal data is collected.

Notices shall explain:

- Identity of the controller
- Purposes of processing
- Lawful basis
- Data recipients
- Retention periods
- Rights of the individual
- Complaint routes

8. PROCESSING VULNERABILITY INFORMATION

Jonathan Smith & Partners recognises that customers may have characteristics of vulnerability which impact their ability to make informed decisions or pursue their financial objectives.

Customers shall be provided with opportunities throughout the customer journey to disclose vulnerability information.

Jonathan Smith & Partners may collect, record, store, use and retain vulnerability information where necessary to:

- Deliver good customer outcomes.
- Prevent foreseeable harm.
- Tailor customer support.
- Meet Consumer Duty obligations.
- Monitor customer outcomes.

Vulnerability information may include:

- Physical health conditions.
- Mental health conditions.
- Disability.
- Bereavement.
- Caring responsibilities.
- Financial resilience concerns.
- Life events.

- Capability and understanding.

Appropriate safeguards shall be implemented at all times.

9. SHARING VULNERABILITY INFORMATION

Where necessary and lawful, vulnerability information may be shared with:

- Lenders.
- Funders.
- Credit Reference Agencies.
- Fraud Prevention Agencies.
- Service providers.

Jonathan Smith & Partners shall ensure:

- A lawful basis exists.
- Sharing is necessary and proportionate.
- Appropriate safeguards are in place.
- Sharing is transparent to customers.

10. CONSUMER DUTY OUTCOME MONITORING

Personal data may be processed to support:

- Customer outcome monitoring.
- Customer understanding assessments.
- Vulnerability monitoring.
- Complaint trend analysis.
- Product reviews.
- Consumer support reviews.
- Foreseeable harm assessments.

Jonathan Smith & Partners shall use Management Information (MI) to identify poor outcomes and implement corrective actions.

Outcome monitoring shall be reported to Senior Management and the Board.

11. CREDIT REFERENCE AGENCIES AND FRAUD PREVENTION

Jonathan Smith & Partners may share personal data with:

- Credit Reference Agencies.
- Fraud Prevention Agencies.
- Identity Verification Providers.

Customers shall be informed through Privacy Notices and customer documentation.

12. AML AND FINANCIAL CRIME PREVENTION

Personal data may be processed to:

- Verify identity.
- Conduct sanctions screening.
- Undertake AML checks.
- Prevent fraud and financial crime.

13. MARKETING AND PECR (Privacy and Electronic Communications Regulations)

Jonathan Smith & Partners shall comply with PECR requirements.

Electronic marketing shall only be undertaken where:

- Valid consent exists; or
- The soft opt-in exemption applies (The *soft opt-in* is a limited exemption under the Privacy and Electronic Communications Regulations (PECR) that allows an organisation to send marketing emails or text messages to an individual without obtaining separate consent, providing all conditions met.)

Marketing preferences shall be maintained and respected.

14. INDIVIDUAL RIGHTS

Individuals have the right to:

- Be informed.
- Access personal data.
- Rectify inaccuracies.
- Erase personal data.
- Restrict processing.
- Data portability.
- Object.
- Challenge automated decision-making.

15. SUBJECT ACCESS REQUESTS

Requests shall:

- Be logged.
- Have identity verified.
- Be responded to within one month.
- Be escalated where complex.

A SAR Register shall be maintained.

16. DATA PROTECTION COMPLAINTS

Jonathan Smith & Partners maintains a dedicated Data Protection Complaints Procedure.

Complaints may relate to:

- Collection of data.
- Use of data.
- Sharing of data.
- Retention of data.
- Security of data.
- Individual rights.

Jonathan Smith & Partners shall:

- Acknowledge complaints promptly.
- Investigate fairly.
- Maintain a Data Protection Complaints Register.
- Identify root causes.
- Implement corrective actions.
- Inform individuals of their right to complain to the ICO.

17. DATA RETENTION

Jonathan Smith & Partners shall maintain a documented Retention Schedule.

FCA regulated records shall normally be retained for a minimum of six years unless a longer retention period is required by law, regulation, insurance requirements or ongoing litigation.

18. THIRD-PARTY PROCESSOR GOVERNANCE

Prior to appointing a processor, Jonathan Smith & Partners shall undertake due diligence covering:

- Information security.
- Cyber security.
- Data protection compliance.
- Operational resilience.
- Regulatory standing.

Appropriate contracts shall be in place before personal data is shared.

19. INTERNATIONAL DATA TRANSFERS

Personal data shall only be transferred outside the UK where appropriate safeguards exist.

20. INFORMATION SECURITY

Jonathan Smith & Partners shall maintain:

- Multi-factor authentication.
- Encryption.
- Access controls.
- Password standards.
- Endpoint protection.
- Backup arrangements.
- Vulnerability management.
- Incident monitoring.

21. DATA BREACH MANAGEMENT

All breaches and suspected breaches must be reported immediately.

Jonathan Smith & Partners shall:

- Maintain a Breach Register.
- Investigate incidents.
- Assess risk.
- Notify the ICO within 72 hours where required.
- Consider FCA notification obligations.
- Implement lessons learned.

Significant incidents shall be reported to the Board.

22. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

DPIAs shall be completed before implementing:

- New CRM systems.
- AI tools.
- Vulnerability monitoring systems.
- Consumer Duty monitoring platforms.
- Lead generation arrangements.
- Large-scale profiling activities.

DPIAs shall be approved by the Data Protection Lead.

23. ARTIFICIAL INTELLIGENCE, PROFILING AND AUTOMATED DECISION-MAKING

Where AI is used, Jonathan Smith & Partners shall ensure:

- Transparency.
- Human oversight.

- Appropriate governance.
- Risk assessments.
- Ongoing monitoring.

Individuals shall be informed:

- How AI is used.
- The purpose of processing.
- The significance of decisions.
- Their right to human intervention.
- Their right to challenge decisions.

24. TRAINING AND AWARENESS

All staff shall receive:

- Induction training.
- Annual refresher training.
- Role-specific training where necessary.

Training records shall be maintained.

25. MONITORING, ASSURANCE AND REPORTING

Jonathan Smith & Partners shall monitor compliance through:

- Internal audits.
- Compliance reviews.
- Management Information.
- Breach reporting.
- Consumer Duty outcome monitoring.
- Third-party oversight.

26. POLICY REVIEW

This policy shall be reviewed annually or following:

- Regulatory change.
- Legislative change.
- Material incidents.
- Significant operational change.
- New technology implementation.