Document Retention Policy

Propertyline (includes Propertyline Letting Ltd and its subsidiaries)

1. Purpose

This Document Retention Policy outlines the guidelines for retaining, archiving, and securely disposing of documents and records within our lettings and estate agency. The purpose is to ensure compliance with legal, regulatory, and business requirements, while also promoting efficient and secure recordkeeping.

2. Scope

This policy applies to all employees, contractors, and agents handling documents in physical or electronic form across all departments of the business, including sales, lettings, property management, finance, and administration.

3. Legal and Regulatory Compliance

The retention and disposal of documents must comply with all applicable legislation, including but not limited to:

- **GDPR (General Data Protection Regulation)**
- **The Data Protection Act 2018**
- **HMRC regulations**
- **The Estate Agents Act 1979**
- **The Housing Act 2004**
- **Anti-Money Laundering (AML) Regulations**

4. Retention Periods

Document Type	Description	Retention Period	Notes
Tenancy Agreements	Signed contracts between landlord and tenant	6 years after end of tenancy	Limitation period for legal claims
Sales Agreements	Contracts for sale of property	6 years after completion	
Client ID and AML Checks	Proof of identity and AML documentation	5 years after end of relationship	As per AML regulations
Property Management Records	Maintenance logs, inspections, repairs	6 years after end of tenancy or management	
Tenancy Applications and References	Including credit and background checks	1 year if not proceeded, 6 years if tenancy commenced	
Financial Records	Invoices, receipts, rent statements, tax-related records	6 years	HMRC requirements

Document Type	Description	Retention Period	Notes
Marketing Materials	Photos, brochures, descriptions	2 years after listing ends	Unless used in dispute resolution
Email Correspondence	Related to lettings/sales	6 years	Where relevant to transactions
Complaints and Disputes	Records of formal complaints and dispute resolution	6 years after resolution	

5. Secure Storage and Access Control
Documents must be stored securely, with appropriate physical and digital access controls in place to prevent unauthorised access, loss, or misuse.

- Physical documents should be kept in locked cabinets in secure areas.
- Digital documents should be stored on encrypted systems with access restricted based on role.

6. Disposal of Records
When records reach the end of their retention period, they must be securely destroyed:

- **Paper records** should be shredded using a cross-cut shredder or via an approved document destruction service.
- **Electronic records** must be permanently deleted, including from backup systems where applicable.

7. Review and Audit
A review of stored records should be conducted annually to ensure compliance with this policy. Any non-compliance or potential risks should be reported to the Data Protection Officer.

8. Responsibilities

- All staff are responsible for following this policy.
- Managers must ensure team compliance.
- The Data Protection Officer (or designated compliance officer) oversees implementation, training, and audits.

9. Policy Review
This policy will be reviewed annually or whenever significant changes to legislation or business operations occur.

Approved by: Mohammed Younis
Position: Director
Date of Approval: 1st October 2025
Next Review Date: 30th September 2026