

INFORMATION SECURITY

Data Retention Policy

Version 1.1



Status	Draft for review
Classification	Restricted
Date Updated	04/09/2026
Version	1.1

This document is classified as RESTRICTED

Document Control

Revision history

Date	Version	Author	Summary of changes
19/02/2024	1.0	Rahim Hankin	Version 1 issued
04/09/2026	1.1	Muji Ali	Reviewed and updated against current legal, regulatory and ISMS requirements

Approvals

Date	Version	Approver name	Approver title
04/09/2026	1.1	Muji Ali	Information Security Lead

Contents

1	About this Policy
2	Scope of Policy
3	Guiding Principles
4	Roles and Responsibilities
5	Types of Data and Data Classifications
6	Retention Periods
7	Storage, Backup and Disposal of Data
8	Special Circumstances and Legal Holds
9	Advice and Questions
10	Breach Reporting and Audit
A	Definitions
B	Record Retention Schedule
B.1	Company and Corporate Records
B.2	Pension Records
B.3	Facilities and Security Records
B.4	IT Records
B.5	Sales, Marketing and Customer Records
B.6	Procurement Records
B.7	Legal Records
B.8	Employment Records
C	Legal and Regulatory References

1. About this Policy

1.1 The corporate information, records and data of FDM UK Limited (FDM) are important to the way we conduct business, demonstrate compliance and manage our Staff Members, customers, suppliers and other stakeholders.

1.2 Legal, regulatory, contractual and business requirements mean that some records must be retained for defined periods. Retaining data for longer than necessary can create information security, privacy, legal and operational risk.

1.3 This Data Retention Policy sets out FDM requirements for retaining, reviewing and securely disposing of data and should be read together with the Record Retention Schedule in Annex B.

1.4 Failure to comply with this policy may expose FDM to regulatory action, contractual or legal risk, unnecessary storage cost, loss of evidence and inappropriate retention of personal or confidential information.

1.5 This policy does not form part of any Staff Member's contract of employment and may be amended as FDM's legal, regulatory, contractual or operational requirements change.

2. Scope of Policy

2.1 This policy applies to all data held or controlled by FDM, whether physical or electronic, including hard-copy documents, contracts, notebooks, correspondence, emails, electronic documents, audio and video recordings, CCTV where controlled by FDM, system logs and other business records.

2.2 It applies to data held by suppliers or cloud services on FDM's behalf and to FDM data processed on approved personal devices or other authorised locations.

2.3 It applies to personal and non-personal data and should be applied alongside FDM information classification, handling, access control, supplier, backup and incident-management requirements.

3. Guiding Principles

3.1 FDM applies the following principles:

- Comply with legal, regulatory and contractual record-keeping requirements.

Keep personal data no longer than necessary for the purpose for which it is processed, in accordance with the [UK GDPR storage limitation principle](#).

- Handle, store, archive and dispose of data securely and in accordance with its classification.
- Retain records where there is a defined legal, regulatory, contractual or business need; do not retain information 'just in case'.
- Apply documented ownership and accountability for retention and disposal.
- Review retention requirements periodically and when laws, systems, suppliers, business processes or risks change.
- Suspend normal disposal where a legal hold, investigation, audit, incident or other approved preservation requirement applies.

4. Roles and Responsibilities

Role	Responsibility
Information Security Lead	Owns this policy, coordinates review of the Record Retention Schedule, maintains ISMS alignment and supports audit and assurance activities.
Data Protection Officer (DPO)	Advises on personal-data retention, storage limitation, data subject rights and other data-protection requirements.
Department / Data Owners	Identify legal, contractual and business retention needs for the records they own; ensure records are classified, reviewed and disposed of when due.
IT / System Owners and Suppliers	Implement technical retention, backup, deletion and recovery arrangements in line with approved FDM requirements and supplier agreements.
All Staff Members	Comply with this policy, the Record Retention Schedule, legal holds and disposal instructions; do not retain duplicate or unnecessary information.

5. Types of Data and Data Classifications

5.1 Formal or official records. Records listed in Annex B are retained because they are required by law or regulation, support contractual or legal rights, provide evidence of transactions or decisions, or are required for the effective operation of FDM.

5.2 Disposable information. Information with no continuing legal, regulatory, contractual or business value should be securely disposed of once its temporary purpose has been served. Examples include:

- Unannotated duplicates of official records.
- Drafts, working notes and worksheets that do not record a material decision or significant stage in creating an official record.
- Reference material obtained from external sources that is no longer required.
- Spam, junk mail and routine transitory communications with no continuing business value.

5.3 Personal data. Personal data may appear in both formal records and disposable information. Retention must comply with the UK GDPR storage limitation principle and any specific legal or regulatory period that applies.

5.4 Confidential information belonging to others. Confidential information received from customers, suppliers, previous employers or other third parties must only be retained and used where FDM is authorised to do so and must be disposed of securely when no longer required.

6. Retention Periods

6.1 Formal or official records. Records listed in Annex B must be retained for the stated period unless an approved legal hold, investigation, contractual requirement or other documented justification requires longer retention.

6.2 Disposable information. Disposable information should be retained only while it has a legitimate business purpose and then securely deleted or destroyed.

6.3 Personal data. FDM must be able to justify the retention period applied to personal data. [ICO storage limitation guidance](#) should be used alongside the statutory and business requirements in Annex B.

6.4 Records not listed in Annex B. If a record is not listed, the relevant Data Owner should determine whether it is disposable or whether a defined retention period should be added to the Schedule, with advice from the Information Security Lead and DPO where appropriate.

7. Storage, Backup and Disposal of Data

7.1 Storage. Data must be stored in approved locations and protected in accordance with its classification, access requirements and the FDM Information Handling Policy.

7.2 Backup and recovery. Backup and recovery arrangements are system-specific and must follow approved FDM or supplier backup, resilience and recovery requirements. Backup copies are not a substitute for the Record Retention Schedule and must not be used to extend normal active retention without a documented reason.

7.3 Secure disposal. Paper records containing confidential, personal or commercially sensitive information must be disposed of using approved confidential-waste or shredding arrangements. Electronic records must be securely deleted or rendered inaccessible using approved technical methods. Disposal by suppliers must be covered by applicable contractual and assurance arrangements.

7.4 Legal hold. Routine deletion and disposal must stop immediately for records subject to a legal hold, investigation, audit, regulatory request or other approved preservation instruction. Normal disposal may resume only when the hold is formally lifted.

8. Special Circumstances and Legal Holds

8.1 Staff Members must preserve records that may be relevant to actual or reasonably anticipated litigation, regulatory or law-enforcement activity, an audit, investigation, incident or material business transaction.

8.2 Preserving records includes preventing deletion or alteration, suspending automated disposal where necessary and maintaining the integrity of electronic and physical records.

8.3 Questions about whether a hold applies should be escalated to the Information Security Lead, relevant management and, where appropriate, the DPO or legal adviser.

9. Advice and Questions

9.1 Questions about retention periods, classification, disposal or exceptions should be raised with the Information Security Lead. Personal-data retention questions should also be referred to the DPO where appropriate.

10. Breach Reporting and Audit

10.1 Suspected inappropriate retention, unauthorised deletion, loss of records, failure to apply a legal hold or other information-security event must be reported promptly to infosec@fdm.uk and handled in accordance with the FDM Security Incident Policy.

10.2 Compliance with this policy may be reviewed through ISMS monitoring, internal audit, supplier assurance, management review and corrective-action activity.

10.3 Staff Members who raise concerns in good faith must not be subject to retaliation. Failure to follow retention, preservation or secure-disposal requirements may be addressed in accordance with applicable FDM procedures.

Annex A - Definitions

Data: All information and records held or controlled by FDM, including physical and electronic records, personal and non-personal data.

Data Owner: The person or function accountable for a category of information, business process or system and for ensuring appropriate retention and disposal.

Data Protection Officer (DPO): The appointed DPO responsible for advising on and monitoring compliance with data-protection obligations.

Data Retention Policy: This policy and its Record Retention Schedule, which define FDM requirements for retaining, reviewing and disposing of data.

Disposable information: Information that can be deleted or destroyed once its temporary purpose has been served because it is not required as an official record.

Formal or official record: A record retained because of a legal, regulatory, contractual, evidential or business requirement.

Legal hold: A requirement to suspend normal destruction or deletion because records may be required for litigation, investigation, audit, regulatory or other approved purposes.

Non-personal data: Information that does not identify a living individual, including information that has been effectively anonymised.

Personal data: Information relating to an identified or identifiable living individual, including special-category data and pseudonymised personal data where the individual remains identifiable.

Record Retention Schedule: Annex B, which sets standard retention periods for defined categories of FDM records.

Storage limitation: The UK GDPR principle that personal data must not be kept in identifiable form for longer than necessary for the purposes for which it is processed.

Annex B - Record Retention Schedule

About this Schedule

FDM establishes retention and destruction periods to support legal and regulatory compliance, protect information and evidence, support contractual rights and control storage and privacy risk.

Staff Members must follow the periods below. Where a statutory or regulatory authority is shown, the authority text is hyperlinked to an official source. A legal hold or other approved preservation requirement overrides routine disposal until the hold is lifted.

B.1 Company and Corporate Records

Type of data	Retention period	Authority / reason	Comments
Accounting and company tax records	6 years from the end of the company financial year to which they relate; longer where an applicable HMRC exception applies.	HMRC company record-keeping requirements Companies Act 2006 s388	The six-year FDM period is used to meet company-tax record-keeping requirements and avoid under-retention.
Register of members / shareholder records	Entries relating to former members: retain for at least 10 years after they cease to be members.	Companies Act 2006 s121	Local registers of directors, directors' residential addresses, secretaries and PSCs were abolished from 18 November 2025 and are not separately listed here.
Minutes of directors' meetings	10 years from the date of the meeting.	Companies Act 2006 s248	
Member resolutions, minutes of general meetings and sole-member decisions	10 years from the date of the resolution, decision or meeting.	Companies Act 2006 s355 Companies Act 2006 s358	
Health and safety inspections, property management and asset records	6 years unless a longer period is required for a specific asset, contract, claim or hazard.	Limitation Act 1980 s5	Six years supports the ordinary limitation period for simple-contract claims; specialist health-and-safety records may require longer retention.
Historical company records and archives of enduring corporate value	Indefinite where there is a documented archival or corporate-history purpose.	Business / archival need	Personal data within archives should be minimised where practicable.

B.2 Pension Records

Type of data	Retention period	Authority / reason	Comments
Automatic enrolment scheme/provider details and employer pension scheme reference	6 years	The Pensions Regulator - keeping records	Minimum statutory period.
Evidence the scheme meets automatic-enrolment requirements	6 years	The Pensions Regulator - keeping records	Minimum statutory period.
Jobholder / worker automatic-enrolment records, including NI number, date of birth and enrolment date	6 years	The Pensions Regulator - keeping records	Minimum statutory period.

Type of data	Retention period	Authority / reason	Comments
Earnings, contributions and contribution-payment records	6 years	The Pensions Regulator - keeping records	Minimum statutory period.
Postponement notices and related worker records	6 years	The Pensions Regulator - keeping records	Minimum statutory period.
Opt-in and joining notices	6 years	The Pensions Regulator - keeping records	Original format or an acceptable copy/electronic version.
Opt-out notices	4 years	The Pensions Regulator - keeping records	Original format or an acceptable copy/electronic version.
Occupational pension scheme tax / administration records within Regulation 18	Tax year to which they relate plus 6 years	Registered Pension Schemes Regulations 2006, reg 18	Minimum statutory period.
Ill-health early-retirement records, including medical reports	While entitlement continues and 15 years after benefits stop	Limitation / evidential need	May also require relevant job-description information.
Death-benefit nomination and revocation records	While entitlement continues and 15 years after the death of the member and beneficiaries	Limitation / evidential need	

B.3 Facilities and Security Records

Type of data	Retention period	Authority / reason	Comments
CCTV recordings controlled by FDM	No longer than necessary for the documented purpose. Where FDM controls routine footage, use a defined local period (normally up to 90 days) unless a shorter period is sufficient; preserve relevant footage for an incident, investigation or claim where required.	UK GDPR storage limitation ICO storage limitation guidance	Where CCTV is controlled by the premises provider, the provider's documented retention period applies subject to supplier assurance.
FDM visitor logs	6 months, unless required longer for a specific incident, investigation, claim or legal hold.	UK GDPR storage limitation	Premises-provider visitor records follow the provider's documented retention arrangement.
Property management and asset agreements	6 years after expiry/breach for simple contracts; 12 years where executed as a deed.	Limitation Act 1980 s5 Limitation Act 1980 s8	
Building contracts executed as a deed	12 years from practical completion	Limitation Act 1980 s8	
Health and safety files for building works	6 years from completion, or longer where a specific statutory or evidential requirement applies	Limitation Act 1980 s5	

B.4 IT Records

Type of data	Retention period	Authority / reason	Comments
Internally developed IT infrastructure, software and systems for internal use	5 years from decommissioning	Business need	Review for anonymisation/minimisation where records contain personal data.
Externally developed IT infrastructure, software and systems	7 years from decommissioning	Contractual / limitation need	See also Procurement Records.
Internally developed IT systems used externally	7 years from decommissioning	Contractual / limitation need	May be relevant to customer claims, service history and disputes.
Security and systems monitoring logs	Current year plus 1 year, unless a documented security, contractual, legal or investigation need requires longer retention	Security / business need	Longer retention should be justified; consider anonymisation where practical.
Business continuity and information-security plans	3 years after being superseded, unless a longer legal/contractual need applies	Business / legal / contractual need	Retain enough history to evidence the control environment and support claims or audit.
Technical support and help-desk requests	3 years after closure / end of the relevant system, subject to any longer contractual or claim need	Business / contractual need	Consider anonymisation where practical.
Technical information relating to external customer user accounts	1 year from account closure, unless a longer contractual or legal need applies	Business / contractual need	
Software licences, support agreements and hardware agreements	Contract period plus 6 years; 12 years where executed as a deed	Limitation Act 1980 s5 Limitation Act 1980 s8	
System backups	Per approved system or supplier backup and recovery schedule	Business continuity / information-security need	Backup copies expire through normal rotation and are not used to extend active record retention unless specifically required.

B.5 Sales, Marketing and Customer Records

Type of data	Retention period	Authority / reason	Comments
Bought-in mailing lists	Up to 1 year, subject to valid provenance, transparency and direct-marketing requirements	PECR 2003 ICO direct marketing guidance	Do not retain or use a list where the lawful marketing basis cannot be demonstrated.
Contracts associated with bought-in mailing lists	Contract period plus 6 years; 12 years for deeds	Limitation Act 1980 s5 Limitation Act 1980 s8	
Marketing database records	2 years from last meaningful contact	Business need	Review suppression requirements before deletion.
Customer relationship / account-history records	6 years from last contact	Business / limitation need	

Type of data	Retention period	Authority / reason	Comments
Order fulfilment records	6 years from completion	HMRC company record-keeping requirements Limitation Act 1980 s5	
Opt-out / suppression lists	Indefinite, but retain only the minimum information required to honour the opt-out	PECR 2003 ICO direct marketing guidance	
Evidence of marketing consent	While consent remains valid and 6 years after withdrawal or cessation where needed to evidence compliance	UK GDPR / PECR	Retention should remain proportionate to the evidential need.
Market research and marketing campaigns	2 years from completion	Business need	
Press releases	5 years from publication	Business / historical need	
Customer complaints	6 years from settlement or closure	Limitation Act 1980 s5	
Website analytics reports derived from cookies	2 years	Business need	Cookie identifiers themselves may have different lifetimes depending on function and consent settings.

B.6 Procurement Records

Type of data	Retention period	Authority / reason	Comments
Unsuccessful tenders	2 years after completion of the tender process	Business need	May be reduced where volume and risk justify a shorter period.
Successful tenders	Contract period plus 6 years; 12 years where executed as a deed	Limitation Act 1980 s5 Limitation Act 1980 s8	
Contractual documents	Contract period plus 6 years; 12 years where executed as a deed	Limitation Act 1980 s5 Limitation Act 1980 s8	

B.7 Legal Records

Type of data	Retention period	Authority / reason	Comments
Legal advice and opinions (non-litigation)	6 years after the life of the service or matter to which the advice relates	Business / evidential need	
Legal advice and records relating to litigation or claims	6 years from settlement or withdrawal, unless legal advice specifies otherwise	Limitation Act 1980 s5	
Data subject rights requests	6 years from closure	Limitation / evidential need	Personal data should be minimised to what is required to evidence handling of the request.
Previous versions of policies	6 years after being superseded	Business / evidential need	Longer retention may be appropriate where relevant to a claim, audit or certification history.

Type of data	Retention period	Authority / reason	Comments
Monitoring and investigation records	6 years from closure, subject to case-specific legal, HR or regulatory requirements	Limitation / evidential need	
Insurance claims	3 years after settlement or longer where required by the insurer or claim circumstances	Contractual / evidential need	

B.8 Employment Records

Type of data	Retention period	Authority / reason	Comments
Recruitment records for unsuccessful applicants (CVs, application forms, interview notes, assessments and equal-opportunities records)	6 months after candidates are notified of the outcome, unless a separate documented lawful basis and retention period applies (for example, an agreed talent pool).	UK GDPR storage limitation ICO storage limitation guidance	Successful-candidate records required for employment may be transferred to the employment file.
DBS certificate information	Normally no longer than 6 months after the recruitment or screening decision; longer only in exceptional justified circumstances.	DBS employer guidance DBS Code of Practice	Do not retain a photocopy or representation of the certificate beyond what is necessary. A limited screening record may be retained separately.
Evidence of completed DBS / financial / background screening for designated high-profile roles	Up to 6 years, or until the employee leaves if earlier, unless a legal hold or other specific requirement applies.	FDM business / evidential need	Retain only the minimum evidence required to demonstrate the check and decision; this is separate from full DBS certificate information.
Right-to-work / immigration checks	Duration of employment plus 2 years, then securely destroy.	Home Office right-to-work guidance	
Employment contracts, written particulars and documented changes	While employment continues and 7 years after employment ends.	Limitation Act 1980 s5	FDM retains slightly beyond the ordinary six-year limitation period.
Collective agreements retained on an employee record	While employment continues and 7 years after employment ends.	Limitation Act 1980 s5	
Payroll, wage, overtime, bonus, expenses and benefits records	At least 3 years from the end of the tax year to which they relate; FDM retains relevant employment/pay records for up to 7 years after employment where needed for pay disputes or claims.	HMRC PAYE record-keeping Limitation Act 1980 s5	
Company accounting / tax records associated with payroll	6 years from the end of the company financial year to which they relate.	HMRC company record-keeping	
National Minimum Wage records relating to hours worked and payments	At least 6 years beginning with the day after the pay reference period following the one covered by the record ends.	National Minimum Wage Regulations 2015, reg 59 GOV.UK employer guidance	

Type of data	Retention period	Authority / reason	Comments
Current bank details	Delete as soon as practicable after employment ends and final payments and any required reconciliations are complete.	UK GDPR storage limitation	
Travel and subsistence records	While employment continues and up to 7 years after employment ends where required for payroll, tax or claims.	HMRC PAYE record-keeping Limitation Act 1980 s5	
Employee loan / season-ticket advance records	While the arrangement is active and up to 7 years after employment ends where required for reconciliation or claims.	Limitation Act 1980 s5	
General personnel records (qualifications, references, performance, disciplinary, grievance, termination and related employment records)	While employment continues and up to 7 years after employment ends, subject to earlier deletion where a shorter period is appropriate.	UK GDPR storage limitation Limitation Act 1980 s5	Apply case-specific retention to sensitive HR information where appropriate.
Working-time opt-out and other records required under regulation 9	2 years from the date the record was made / relevant period.	Working Time Regulations 1998, reg 9	
Annual leave and holiday-pay compliance records	6 years from the date the record was made.	Employment Rights Act 2025, s35 GOV.UK holiday-pay record guidance	Requirement applies from 6 April 2026.
Statutory maternity pay / maternity absence records	3 years from the end of the tax year to which they relate.	HMRC maternity record-keeping guidance	
RIDDOR reportable accident, disease and dangerous-occurrence records	At least 3 years from the date of the report / incident record, subject to longer retention where required for a claim, insurer, legal hold or specialist health-and-safety requirement.	HSE RIDDOR guidance HSE record-keeping guidance	Specialist exposure records (for example asbestos or other hazardous substances) may require materially longer periods and should follow the applicable specific law.

Annex C - Legal and Regulatory References

The hyperlinks below are provided to support maintenance and audit of this policy. They point to official legislation, regulator or government guidance current at the date of this review. FDM should re-check them when the policy is reviewed or when relevant law changes.

Reference	Relevance	Official link
UK GDPR Article 5(1)(e) - storage limitation	Core personal-data retention principle.	Open official source
ICO - Storage limitation	Regulatory guidance on setting, reviewing and justifying retention periods.	Open official source
Data Protection Act 2018	UK data-protection legislation supporting the UK GDPR framework.	Open official source
Companies Act 2006 s121	Register of members / former-member entries.	Open official source
Companies Act 2006 s248	Retention of directors' meeting minutes.	Open official source
Companies Act 2006 ss355 and 358	Company resolutions and meeting records.	Open official source
Companies Act 2006 s388	Accounting records retention provisions.	Open official source
GOV.UK - Company and accounting records	Six-year company tax/accounting record-keeping requirement.	Open official source
Economic Crime and Corporate Transparency Act 2023 s51	Abolition of local registers of directors, residential addresses, secretaries and PSCs.	Open official source
Limitation Act 1980 s5	Six-year limitation period for simple-contract claims.	Open official source
Limitation Act 1980 s8	Twelve-year limitation period for specialty/deed claims.	Open official source
The Pensions Regulator - Keeping records	Automatic-enrolment record retention, including six-year and four-year periods.	Open official source
Registered Pension Schemes (Provision of Information) Regulations 2006, reg 18	Pension scheme record retention.	Open official source
National Minimum Wage Regulations 2015, reg 59	National Minimum Wage records.	Open official source
GOV.UK - Employers and the minimum wage	Current six-year NMW record-keeping guidance.	Open official source
Working Time Regulations 1998, reg 9	Working-time compliance records.	Open official source
Employment Rights Act 2025, s35	Six-year annual leave / holiday-pay record-keeping duty.	Open official source
GOV.UK - Holiday pay	Current annual-leave and holiday-pay record guidance.	Open official source
Home Office - Employer's guide to right-to-work checks	Duration of employment plus two years retention for right-to-work evidence.	Open official source
PAYE records	3-year statutory retention.	Open official source
GOV.UK - Statutory Maternity Pay record keeping	Three-year maternity record-keeping requirement.	Open official source
HSE - RIDDOR	Incident reporting and record-keeping requirements.	Open official source
DBS - Employer guidance	Storage, retention and disposal of DBS certificate information.	Open official source

Reference	Relevance	Official link
DBS Code of Practice	Code governing registered bodies and recipients of DBS information.	Open official source
Privacy and Electronic Communications Regulations 2003	Electronic direct-marketing and cookie-related obligations.	Open official source
ICO - Direct marketing guidance	Regulatory guidance on direct marketing, consent and suppression.	Open official source