Data Retention & Disposal Policy

Policy · UK · Updated 2026-07-11 · Square brackets are placeholders to replace with your own details.

A data retention and disposal policy sets out how long your organisation keeps each type of record containing personal data, why, and how records are securely destroyed when the time is up. It pairs a short set of rules with a retention schedule — the table your team actually uses.

Keeping everything forever feels safe but is the opposite: every record you hold is one more you must protect, search when a subject access request arrives, and account for if there is a breach. Old data is pure liability with no operational value.

This template gives you the policy rules, a retention schedule to complete by record type, secure disposal standards, and the legal-hold mechanism that pauses destruction when a dispute or investigation is live.

Purpose and scope

This policy sets out how long [Your company] retains records containing personal data and how they are disposed of. It applies to all records in all formats — databases, files, emails, paper, backups, and archives — and to all staff who create or manage them.

Policy statement

[Your company] keeps personal data only as long as it is needed for a documented purpose, retains it for the periods in the schedule below, and disposes of it securely when the period ends. No one keeps personal copies, exports, or shadow spreadsheets outside the systems of record.

Responsibilities

- Policy owner ([name/role]): maintains this policy and the retention schedule, and decides legal holds.
- Record owners ([role per area, e.g. office manager for HR files, finance lead for accounts]): apply the schedule to their records and run periodic disposal.
- All staff: save records to the systems of record, not local drives, and flag records with no apparent owner or period.

How retention periods are set

- Legal or regulatory requirement: where legislation sets a period — tax and payroll records, for example — that period applies. Record the source; check current official guidance rather than folklore.
- Potential claims: some records are kept for the period during which a legal claim could realistically arise — take advice or check official guidance rather than guessing.
- Operational need: everything else is kept only as long as it is actually used, and the reason is written in the schedule.
- Where only statistics are needed long term, data is anonymised instead of retained.

Retention schedule

- Customer accounts and transaction records: [period] from the end of the relationship. Reason/source: [complete].
- Enquiries and prospect data: [period] from last contact. Reason/source: [complete].
- Financial, tax, and payroll records: [period — set by tax legislation; check current official guidance]. Reason/source: [complete].
- Staff records: [period] after employment ends; unsuccessful applicant records: [period] after the decision. Reason/source: [complete].
- Accident and incident records: [period]. Reason/source: [complete].
- CCTV footage: [period — typically short] unless preserved for an incident. Reason/source: [complete].
- Emails and general correspondence: [approach, e.g. deleted or archived after (period) unless filed as a record]. Reason/source: [complete].

Secure disposal

- Paper records are cross-cut shredded or placed in confidential waste via [provider] — never in general waste.
- Digital records are deleted from the system of record and any copies on shared drives; deletion is confirmed by the record owner.
- Devices being retired are securely wiped or destroyed via [certified provider], with certificates kept.
- When a contract with a software or service provider ends, [name/role] confirms in writing that our data has been deleted or returned.
- Disposals of whole record classes are logged: what, when, by whom.

Legal holds

If litigation, an investigation, a complaint, or a subject access request is live or reasonably expected, [name/role] declares a legal hold: routine destruction stops for all records in scope, and the affected record owners are told in writing. The hold overrides the schedule until [name/role] lifts it in writing.

Records and review

The schedule, disposal logs, and hold notices are kept at [system/location]. This policy and the schedule are reviewed [frequency, e.g. annually] and whenever we adopt new systems, new record types, or new legal obligations. Owner: [name/role]. Next review due: [date].

How to use this template

1. Inventory what you actually hold before touching the schedule — walk the shared drives, filing cabinets, and system exports first.
2.

Complete the reason/source column for every row; a period with no justification is the first thing that fails scrutiny.

3. Check periods set by other legislation — tax, payroll, health and safety — against current official guidance, not memory.
4. Assign a named record owner to every row, then diarise the first disposal run.
5. Do one supervised disposal run within a month of adopting the policy — the backlog is where the risk lives.
6. Cross-reference the schedule in your privacy policy and employee privacy notice so all three documents agree.

Official guidance

› ICO — UK GDPR guidance and resources