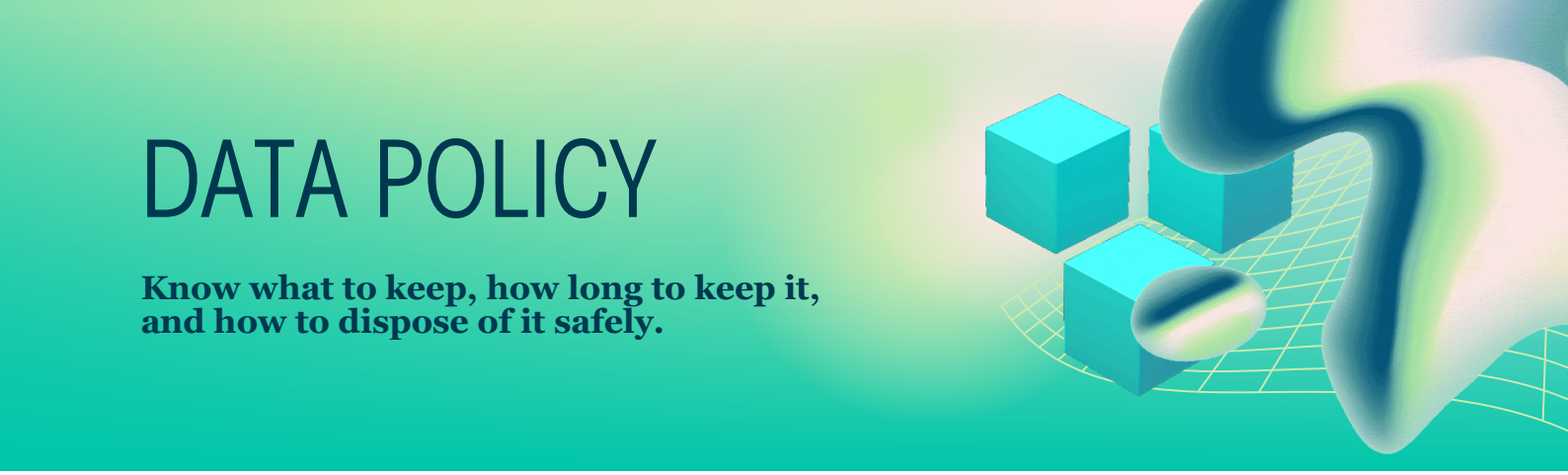

Small Business Data Retention and Disposal Policy Template (2026 Edition)

This template helps you:

- **Keep what you need**
- **Remove what you don't**
- **Reduce exposure in case of a breach**

SECTION 1 — Policy Overview (Fill This Out)

Company Name: _____
Policy Owner: _____
Effective Date: _____
Last Reviewed: _____

Purpose:
This policy defines how our business retains, protects, and securely disposes of data to reduce risk, support operations, and meet legal and business requirements.

SECTION 2 — Data Categories (Define What You Have)

Check all that apply:

☐ Customer Data (names, contact info, records)
☐ Financial Data (payments, invoices, banking)
☐ Employee Data (HR files, payroll, IDs)
☐ Email and Communications
☐ Operational Data (documents, internal files)

□ Vendor and Partner Data
□ Marketing Data

Why this matters:
You can't protect or manage data if you don't know what exists.

SECTION 3 — Data Retention Guidelines

Data Type	Retention Period	Storage Location	Owner
Customer Data	_____ years	_____	_____
Financial Records	_____ years	_____	_____
Employee Records	_____ years	_____	_____
Email	_____ months/years	_____	_____
Operational Files	_____ months/years	_____	_____

Why this matters:
Keeping data longer than necessary increases risk and liability.
Too short can disrupt operations or compliance.

SECTION 4 — Access and Protection Rules

□ Access is limited based on job role
□ Sensitive data is encrypted or protected
□ MFA is required for systems storing sensitive data
□ Data is not stored on personal devices unless approved

Why this matters:
Data retention is not just about storage, it's about controlling who can access it.

SECTION 5 — Backup and Recovery Considerations

□ Critical data is backed up regularly
□ Backup retention aligns with business needs
□ Old backups are reviewed and cleaned up
□ Backup access is restricted

Why this matters:
Backups often contain old data that is forgotten but still exposed.

SECTION 6 — Data Disposal Methods

Digital Data

□ Files are permanently deleted (not just moved to trash)
□ Storage devices are wiped before reuse
□ Cloud data is removed from active and backup systems when required

Physical Data

□ Paper records are shredded
□ Storage devices are destroyed or wiped
□ Old hardware is securely disposed of

Why this matters:
Improper disposal is a common source of data leaks.

SECTION 7 — Trigger Events for Data Deletion

□ Retention period expires
□ Employee leaves the company
□ Customer relationship ends
□ Legal or compliance requirements are met
□ Data is no longer needed for business operations

Why this matters:
Deletion should be tied to events, not random decisions.

SECTION 8 — Responsibilities

Management:

- Approves retention timelines
- Ensures policy is followed

Employees:

- **Store and handle data correctly**
- **Report issues or concerns**

IT / Support:

- **Enforces access controls**
- **Manages backups and disposal**
- **Monitors compliance**

Why this matters:
A policy without assigned responsibility is not enforceable.

SECTION 9 — Review and Updates

□ Policy is reviewed annually
□ Changes in business operations are reflected
□ New systems or tools are included

Why this matters:
Data practices change. Policies must keep up.

SECTION 10 — Quick Compliance Check

Ask yourself:

Do we know what data we store?
Do we know how long we keep it?
Do we remove data we no longer need?
Can we prove we follow this policy?

If any answer is "no," this policy needs attention.

Quick Rule of Thumb

If you don't need the data… don't keep it.