



Data Retention Policy

1. Purpose and Scope

This policy sets out how SmartCarbon Limited ("SmartCarbon", "we", "us", "our") retains and disposes of personal data and business information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other applicable laws.

The purpose of this policy is to:

- Ensure data is kept for no longer than is necessary.
- Comply with legal, contractual, and regulatory requirements.
- Protect the privacy and rights of individuals.
- Manage storage costs and reduce risk associated with holding unnecessary data.

This policy applies to:

- All employees, contractors, and consultants of SmartCarbon.
- All formats and types of data, whether paper or electronic, including emails, databases, files, and cloud-stored information.

2. Principles of Data Retention

SmartCarbon follows these core principles:

1. **Purpose limitation** – Data is retained only for the purposes for which it was collected.
 2. **Minimisation** – We keep only the data that is necessary for operational, contractual, or legal reasons.
 3. **Time limitation** – Data is deleted or anonymised when it is no longer needed.
 4. **Security** – Retained data is stored securely and access is restricted to authorised personnel.
-

3. Retention Periods

The following retention periods apply unless a different period is required by law, regulation, or contractual obligation:

Data Type	Retention Period	Reason
Client contracts and project deliverables	7 years from contract end date	Legal limitation period for contractual claims
Financial records (invoices, receipts, tax documents)	7 years	HMRC requirements
Carbon footprint datasets provided by clients	3 years from project completion unless otherwise agreed	Support for follow-up analysis, audit trails
Client contact details	While relationship is active + 2 years	Business continuity and relationship management
Staff employment records	6 years after employment ends	Legal and employment law requirements
Recruitment records (unsuccessful applicants)	6 months	GDPR guidance
Email correspondence	2 years unless relevant to ongoing projects or legal matters	Storage management
Health and safety records	3 years (general) / 40 years (where involving hazardous substances)	HSE requirements
Marketing data (mailing lists, consent forms)	Until consent withdrawn or inactive for 2 years	GDPR consent rules

4. Secure Disposal and Deletion

When data is no longer required:

- **Electronic data** will be securely deleted from all systems, including backups where feasible.
- **Paper records** will be shredded or destroyed using a secure disposal service.
- **Third-party processors** must provide written confirmation of secure disposal when acting on our behalf.

5. Responsibilities

- **Data Protection Lead** – Operations Director - Ensures compliance with retention requirements and oversees annual reviews.
- **All employees** – Follow retention guidelines and dispose of data securely.
- **IT providers** – Maintain secure deletion processes and assist with removal from systems.

6. Review of Policy

This policy will be reviewed **annually** in line with our Cyber Security Essentials certification or sooner if there are significant changes to legislation, business operations, or contractual obligations.

Approval & Version Control

- **Owner:** Operations Director, Graeme Mills
- **Version:** 1.3
- **Approval Date:** 08/11/2025
- **Next Review:** 08/11/2026

Signed:

A handwritten signature in blue ink, appearing to read 'G Mills', is written over a faint, light blue circular watermark background.

Graeme Mills, Operations Director

Date: 08/11/2025