BRUCKLAY GARAGE LTD
DATA RETENTION & DISPOSAL POLICY

This document aims to outline the Data Retention Policy of Brucklay Garage Ltd (further: the Company), its rights and responsibilities under General Data Protection Regulation, including the Data Retention and Investigatory Powers Act.

1. Introduction

The Company requires to gather personal information and data from individuals and companies which are recorded both electronically and through hard copies. This data is required to be stored in order for the continuing operations of the business and to ensure the Company is adhering to relevant regulations.

Data stored by the Company includes (but is not limited to):

- Personal names and addresses.
- Contact details including phone numbers and email addresses.
- Personal images through CCTV for security purposes.

Data can be gathered from customers, staff and suppliers in the course of routine business requirements. It is often necessary for the Company to retain and store data for monthly business accounts and operational record keeping needs. The untimely deletion of such data could cause the Company's operation and reputation to suffer, lead to a reduced service to customers and harm the Company's ability to adhere to relevant legislation and obligations.

However, the Company recognises the importance of ensuring that data is to be kept up-to-date but not to be held for a period of time that is unnecessary and has potential to affect the rights of those whose data it holds. Data should be held in a responsible and secure manner and the Company affirms to ensure all is done to keep personal information secure.

This Data Retention & Disposal Policy was created and adopted in May 2018 by the Director and employees of the Company. It will be implemented on a day-to-day basis while adhering to relevant policies and procedures.

2. Purpose and Responsibilities

The purpose of this policy is to set out the length of time that the Company records should be retained and the process of disposing of records and data at the end of the period of retention.

It will be the responsibility of the director(s) and employees of the Company going forward to adopt and implement this policy and the Company's Privacy Policy.

3. Retention Policy

Decisions relating to the retention and disposal of data should be guided by Appendix 1 (Data Retention Schedule). Where no relevant guidance is given data should be retained for a maximum period of 5 years (or for any duration that is required under law relating to the particular data) and revision of the Data Retention Schedule should take place at the director(s) discretion.

Once the time period has lapsed for the retention of data it will be up to the director(s) of the Company to determine if the retention of the data should be extended. This may happen for the following reasons:

- The willing consent of the individual or company to allow their holding of the data to be extended.
- The Company believe the data is required to prove compliance with legal obligations.
- The Company require the data for its legal right for potential court proceedings.
- Where the individual or company is in arrears.
- Where the director(s) can prove legitimate business reasons under relevant legal frameworks.
- Where the director(s) can prove relevant business reasons under warranty/guarantee requirements.

3.1 Retention of Paper Documents

Paper documents are still a vital source of data gathering for the Company. Examples include:

- Account application forms
- Machinery Sales and Service Records
- Invoices and Statements
- Customer enquiries
- Staff details

Paper documents should be held in a safe and secure manner so as to ensure the privacy and protection of the individual or company. Paper documents should, where possible be filed appropriately and where confidential, measures should be taken to ensure its safe retention.

3.2 Electronic Documents

Electric documents relating to the Company include:

- Customer details
- Invoices and Statements
- Machinery Sales and Service records
- Emails
- Staff details

Electronic data that contains personal information should only be accessed through software that requires the user to enter a secure password. Electronic data relating to accounts to the Company should also be backed-up on hard drive and done so securely and safely.

All non-confidential data electronically can be stored without the need for passwords.

3.3 CCTV

CCTV images are recorded on the premises for the safety and securing of customers, staff and for business operations. Images are recorded on a 24 hour basis through all public areas of the building (excluding private areas including toilets).

4. Disposal Policy

The disposal of data should take place when the retention period of the data held by the Company expires. This should be done after the relevant director(s) or employees of the Company have assessed through this policy and the Privacy Policy that no extension has either been granted or is deemed necessary under the framework outlined in this document.

4.1 Disposal of Paper Documents

Disposal of paper documents should be done in a way that maintains the confidentiality of the individual or company. Documents containing confidential or personal information should be disposed of either through the use of shredder, waste paper bins after details can no longer be read or destroyed by incineration.

Disposal of non-confidential documents can be done through normal waste or recycling bins.

4.2 Disposal of Electronic Documents

Electronic documents and data that are kept should be reviewed where possible and deleted if no longer in use. A system should be put in place, based on the Retention Schedule to decide if customer details are no longer required to be kept. Where it is deemed that the data is no longer required this should be deleted in a safe and secure manner as to preserve the privacy of the individual or company.

Emails may be archived where they are deemed to be of business purposes and the deletion of said emails may harm the reputation, legal rights and responsibilities or business operation of the Company.

4.3 CCTV

CCTV images are over written after a set period of time (this will not be disclosed as to protect the business). This time period will be deemed to not exceed the rights of individuals who are filmed.

Footage may be stored where the Company believe it has need for the footage to protect its reputation, legal right, in the preparation or during court proceedings or where the Company is asked for the footage by a third party, namely the Police.

CCTV images that are saved will be done so on a secure device and the back-up of the images held in a secure and safe location. If requested this footage will be passed to a third party, namely the Police, whose responsibility it will be to ensure the secure handling and retention of the data.

5. Further Information

The Company takes its responsibilities under data protection regulation seriously. It understands the need to ensure the safe and secure handling and retention of individual and company data. The Company, its director(s) and employees will do all it can to ensure this Policy and the Privacy Policy are upheld, enacted upon and reviewed where necessary.

Further information may be obtained by speaking directly to director(s) of the Company.

This Policy should be read in conjunction with the Company's Privacy Policy, which is available on request or obtained on the Company's website.

This Policy was created in May 2018 and it is for the director(s) to ensure its review.

Appendix 1

Data Retention Schedule

This Data Retention Schedule is given as an illustrative purpose and not all documents held by the Company may be included.

Financial Records

Data Category	Retention Period	Retention Reason
Payroll records	7 years after audit	Financial Requirement
Supplier records	Duration of contracts + 5 years	Business Purpose
Financial Statements	Permanent	Financial Requirement
Invoices and Credits	7 years after audit	Financial Requirement
Business Expenses	7 years after audit	Financial Requirement
Debit/Credit Card receipts	2 years	Financial Requirement
Petty Cash receipts	1 year	Financial Requirement
Bank Deposit Slips	7 years	Financial Requirement
Investments	3 years after investment matures	Financial/Business Requirement
Working Cashbook	10 years	Business Requirement
Customer account records	Duration of active account + 7 years after audit	Financial Requirement

Business/Customer Records

Data Category	Retention Period	Retention Reason
Customer account Details	Duration of active account + 5 years	Business Purpose (added time for product warranty period)
Supplier Details	Duration of active accounts + 5 years	Business Purpose (added time for settlement of warranty/guarantees
Machinery Customers	5 years after expiry of signed data statement agreement	Business Purpose
Customer Contacts	Duration of active accounts + 5 years	Business Purpose (added time for product warranty period)

Employee Records

Data Category	Retention Period	Retention Reason
Personal Information	Duration of employment	Business/Legal/HR Requirements
Disciplinary proceedings	As per legal requirements	Legal/HR Requirements
Job Application/Interview notes where unsuccessful	Deleted immediately	HR Requirement
Job Application/interview notes where successful	Duration of employment	Business/HR Requirement
Payroll/Salary etc	Duration of employment	Financial Requirement
Job history, contract details, pension estimates etc	As per legal requirement	Business/Legal/HR Requirement
Bank Details – Current	Duration of employment	Financial Requirement
Annual Leave records	Duration of employment	HR/Business Requirement
Accident Details	As per legal requirement	HR/Legal Requirement
Parental Leave	As per legal requirement	HR/Legal Requirement
Certificates/Illness records/Sick pay records	As per legal requirement	HR/Legal/Financial Requirement
Redundancy details	As per legal requirement	HR/Legal Requirement
Training details	Duration of employment	HR Requirement

Electronic Records

Data Category	Retention Period	Retention Reason
Emails	Kept for 3 years where relevant	Business Purpose
Archived Emails	15 years	Business Purpose
Machinery Records	5 years after expiry of signed data statement agreement	Business Purpose
Customer details	Duration of active accounts + 5 years	Business Purpose (added time for product warranty period)
Supplier details	Duration of active accounts = 5 years	Business Purpose (added time for product warranty/guarantees)

IT

Data Category	Retention Period	Retention Reason
Recycle Bins	Cleared Monthly	Business Purpose
Downloads	Employee Discretion under Policy terms	Business Purpose
Inbox	Employee Discretion under Policy terms	Business Purpose
Deleted Emails	6 months	Business Purpose
USB Drives	Depending on data held – refer to schedule	Business Purpose