

**DATA RETENTION POLICY WITH SCHEDULE
of
GROUP RETREATS LIMITED**

Introduction

As part of the day-to-day running of our business, we collect and process personal data from a variety of sources. This personal information is collated in several different formats including letters, emails, legal documents, employment records, operations records, images and statements. The personal data is stored both as a hard copy and in electronic form.

Aims of the policy

Our business will ensure that the personal data that we hold is kept secure and that it is held for no longer than is necessary for the purposes for which it is being processed. In addition, we will retain the minimum amount of information to fulfil our statutory obligations and the provision of goods or/and services – as required by data protection legislation, including the General Data Protection Regulation (GDPR).

Retention

This retention policy (along with its schedule), is a tool used to assist us in making decisions on whether a particular document should be retained or disposed of. In addition, it takes account of the context within which the personal data is being processed and our business practices.

Decisions around retention and disposal are to be taken in accordance with this policy.

As and when the retention period for a specific document has expired, a review is always to be carried out prior to the disposal of the document. This does not have to be time-consuming or complex. If a decision is reached to dispose of a document, careful consideration is to be given to the method of disposal.

Responsibility

The Managing Director is responsible for keeping this retention schedule up to date in order to reflect changing business needs, new legislation, changing perceptions of risk management and new priorities for our business.

The Managing Director is responsible for determining (in accordance with this Policy) whether to retain or dispose of specific documents.

The Managing Director may delegate the operational aspect of this function to the Office Manager

The Office Manager should inform The Managing Director if there is any doubt about the minimum retention periods or if the retention of a document is necessary for a potential claim.

Disposal

Our business must ensure that personal data is securely disposed of when it is no longer needed. This will reduce the risk that it will become inaccurate, out of date or irrelevant.

The methods of disposal are to be appropriate to the nature and sensitivity of the documents concerned and include:

- Non-Confidential records: place in waste paper bin for disposal
- Confidential records: shred documents
- Deletion of Computer Records
- Transmission of records to an external body
- Cloud storage

The retention period that we have assigned to each type of record can be found via our website, groupretreats.co.uk. This will be adhered to wherever possible, although it is recognised that there may be exceptional circumstances which require documents to be kept for either shorter or longer periods.

Exceptional circumstances should be reported to The Managing Director without delay.

Date created: 08/11/2024

Date of review: 08/11/2025

Appendix 1: Document retention schedule

Employment records

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
PAYE records	3 years from end of fiscal year	External Supplier	Employment	External Supplier
Maternity and paternity pay records	3 years from end of fiscal year	External Supplier]	Employment	External Supplier
Medical and health records	30 years after employment ceases	Shared Hard Drive	Audit Trail	Secure Deletion
Unsuccessful candidates	6 months after last action	Job Portal	Reference	Job Portal Deletion
Accident report forms	3 years after last action	Shared Hard Drive	Legal	Secure Deletion
Parental leave records	5 years from birth of child	Shared Hard Drive	Legal	Secure Deletion
Employment records: redundancy, equal opportunities; health & welfare records	6 years after last action	Shared Hard Drive	Legal	Secure Deletion
Employees that left the business: emergency contacts and bank account details	Delete immediately after making final salary payment	Shared Hard Drive	Health & Safety	Secure Deletion
Pay & tax: pay deductions, tax forms, payroll, loans	6 years after last action	External Supplier	Employment	External Supplier
Records of formal disciplinary actions in employee file	6 years after last action	Shared Hard Drive	Employment	Secure Deletion
Records of formal grievances in employee file	6 years after last action	Shared Hard Drive	Employment	Secure Deletion

Commercial contracts:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Contracts with suppliers	6 years after last action	Shared Hard Drive	Supply Contract	Secure Deletion
Contracts signed as a deed	12 years after last action	Shared Hard Drive	Legal Contract	Secure Deletion
Guarantees and indemnities	6 years from date of expiration	Shared Hard Drive	Legal	Secure Deletion
Purchase orders and invoices	7 years after last action	External Supplier	Accounting	External supplier

Marketing records:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Mailing lists	1 year after last action	CRM	Audit/Marketing	Secure Deletion

Tax and Accounting Records:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Tax returns	10 years from end of fiscal year	Secure Hard Drive	Audit	Secure Deletion
Accounting & financial management information	6 years from end of fiscal year	Shared Hard Drive	Audit Trail	Secure Deletion
Stock transfer forms and share certificates	20 years from purchase	Shared Hard Drive	Audit Trail	Secure Deletion

Operational records:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Vehicles	Keep asset and depreciation records for 6 years after end of financial year to which they relate	Secure Hard Drive	Audit	Secure Deletion
Closed circuit television recordings	Destroy 4 weeks from the date recorded except where required as evidence	Cloud storage/Secure Hard Drive	Crime Prevention/Audit	Secure Deletion
Fire Risk Assessments	Retain until superseded	Secure Hard Drive	Audit	Secure Deletion
Policies/Procedures	7 years	Secure Hard Drive	Audit	Secure Deletion
Complaints	6 years from end of fiscal year	Secure Hard Drive	Audit	Secure Deletion
Building (i.e. lease/deeds)	Destroy 6 years after property is no longer occupied	Secure Hard Drive	Audit	Secure Deletion
Maintenance contracts	15 years from last action	Secure Hard Drive	Audit	Secure Deletion
Website FAQs	6 months from last action	Secure Hard Drive	Audit	Secure Deletion
Property plans and surveys	25 years	Secure Hard Drive	Audit	Secure Deletion
Insurance schedules	10 years after last action	Secure Hard Drive	Audit	Secure Deletion
Pat tests, fire hazard tests	6 years from last action	Secure Hard Drive	Audit	Secure Deletion
Register of members	Life of company	Secure Hard Drive	Audit	Secure Deletion
Memorandum of association	Life of company	Secure Hard Drive	Audit	Secure Deletion
Register of directors and secretaries	Life of company	Secure Hard Drive	Audit	Secure Deletion
Employer's liability insurance certificates	Life of company	Secure Hard Drive	Audit	Secure Deletion

Intellectual property records:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Copyright material	50 years from expiry	Secure Hard Drive	Audit	Secure Deletion

Email records:

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Email correspondence	Archive emails after 6 months	Email storage	Audit	Archived within Microsoft Office