# Data Retention Policy

# Purpose

The purpose of this policy is to ensure that <Client> complies with the Data Protection Act in respect of the data held about individuals. It serves to protect customers, stakeholders, and staff and to protect us from the consequences of a breach of its responsibilities. It outlines the data held and the designated data retention period and how data will be disposed of when the retention period ends.

Information held for longer than is necessary carries additional risk and cost to the business. Records and information should only be retained when there is a business need to do so. Under UK GDPR and the DPA 2018, personal data processed by <Client> must not be retained for longer than is necessary for its lawful purpose.

# Scope

This applies company wide and applies to all workers (employees, temporary workers, or contractors).

It refers to all information which is used and held within <Client>. Personal Data as defined by GDPR.

# Data Protection

<Client> operates an ISO certified Information Security Management System (ISMS) 27001 which ensures the business protects and manages information securely, through effective risk management.

# Data Disposal

<Client> and its employees will, on a regular basis, review all data, whether held electronically on devices or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant (refer to the Data Retention Matrix).

Once the decision is made to dispose according to the Data Retention Schedule, the data should be deleted, shredded, or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document (see Destruction Method below).

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the <Client> subcontracts for this purpose.

# Retention General Principle

In the event, for any category of documents not specifically defined in the Data Retention Matrix and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document .

# Routine Disposal Schedule

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are document’s which are labelled as Internal Use Only or Public for example, advertisements, flyers, newsletters, meeting requests, routine information requests etc.

# Destruction Method

In Strictest Confidence documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents through an approved disposal firm should be evidenced by proof of destruction.

In Confidence documents are proprietary documents that contain confidential information such as parties’ names, signatures, and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into secure disposal bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Internal Use Only & Public documents are those that do not contain any confidential information or personal data and are published <Client> documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

# Data Retention Matrix

The table below lists the principal documentation which <Client> keep, together with details of statutory retention periods and recommended retention periods. Where the statutory and recommended retention periods differ, the longer period should be followed (which in all cases should be the recommended period).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Description**  | **Record Owner**  | **Retention Period**  | **Start of the Retention Period**  | **Relevant Legal Provision**  |
| **General Company Documents - retention of company accounts, books and accounts and records**  | Finance  | Minimum of 3 years  | The date the document was created  | Section 388(4)(a)(b) Companies Act 2006  |
| **Records and documents of the dissolved legal entity**  | Finance  | It is recommended that membership records be retained for 20 years  | The date of the dissolution of the legal entity  | N/A  |
| **Board Meeting Minutes & Resolutions**   | Board  | Minimum 10 years  | Date of the meeting  | Section 248 Companies Act 2006  |
| **Budgets, Forecasts and internal finance reports**  | Finance  | Current financial year plus 3 years   | The date the document was issued  | N/A  |
| **Annual Reports and accounts**  | Finance  | Permanently  | The date the document was issued  | N/A  |
| **Corporate Income Tax and Accounting Records**   | Finance  | Minimum of 6 years  | The date the document was created  | Section 12B, Taxes Management Act 1970, Paragraph 21, Schedule 18, Finance Act 1998  |
| **VAT Records**   | Finance  | Minimum of 6 years  | The date the document was created  | Paragraph 6, Schedule 11, VAT Act 1994 and HMRC Notice 700/21 (October 2013)  |
| **Purchase Orders and purchase requisitions**   | Finance  | Minimum of 6 years  | The date on the document  | N/A  |
| **HR / Employment Records including identification records**  | HR  | Maximum 6 years after employment ceases  | The date the document was created  | Section 5 Limitation Act 1980 and Data Protection Act 1998  |
| **Payroll and Salary Records**   | Payroll  | Minimum period of six years, following the employee’s termination date  | The financial year in which payments are made  | Schedule 18, paragraph 21, Finance Act 1998, Taxes Management Act 1970.  |
| **Retirement Pensions scheme -  notifiable events, for example, relating to incapacity**  | HR  | 6 years from the end of the scheme year in which the event took place.  | The date of notifiable event  | The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)  |
| **Document Description**  | **Record Owner**  | **Retention Period**  | **Start of the Retention Period**  | **Relevant Legal Provision**  |
| **Employee Pension Records**  | HR  | minimum storage time of six years up to 12 years before disposal  | Date the policy started  | The Registered Pension Scheme (Provision of Information) Regulations 2006 (No. 18)  |
| **Employee right to work checks**  | HR  | Home Office recommended practice is 2 years after employment ends.  | The date of the check  | N/A  |
| **Employee CV’s, application forms and interview notes, references**  | HR  | Retain the data for a minimum of six months, dispose of the data prior to twelve months  | The date the document was received  |   |
| **PAYE Records - Income tax and NI returns, income tax records and correspondence with HMRC**  | Payroll  | Minimum of 3 years  | The end of the financial year to which the records relate  | The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).  |
| **Employee working time records** i**ncluding overtime, holiday, jury service, time off for dependents etc…**   | Payroll  | 2 years from date on which they were made.  | The date of the working time  | The Working Time Regulations 1998 (SI 1998/1833).  |
| **National minimum wage records**  | Payroll  | Minimum of 3 years after the end of the pay reference period following the one that the records cover.  | The end of the pay reference period following the one that the records cover.  | National Minimum Wage Act 1998.  |
| **Employee statutory sick pay records**  | Payroll  | maximum 6 years after the employment ceases.  | Date employment ceases  | N/A - The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55)  |
| **Medical / Safety Records**   | HR  | Maximum 6 years after employment ceases   | The date the document was created  | Section 5 Limitation Act 1980 and Data Protection Act 1998  |
| **First aid and Fire warden training**  | HR  | Minimum of 6 years after employment  | From date of lats training  | Health and Safety (First Aid) Regulations 1981 and ire Precautions (Workplace) Regulations 1997.  |
| **Accident reports and books**   | HR  | Minimum 3 years from date of last entry .  | The date the report was made  | Regulation 12, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013/1471  |
| **Maternity Pay Records -** **calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)**  | HR  | Minimum of 3 years after maternity ends  | The end of the tax year in which the maternity pay period ends  | Regulation 26, Statutory Maternity Pay, (General) Regulations 1986 (SI 1986/1960)  |
| **Registered information concerning the recycling or disposal of waste materials**  | ISO Manager  | Minimum 3 years Minimum 2 years   | The date when the shipment starts The date of the transfer   | Article 20 of the Regulation (EC ) No 1013/2006 on Shipments of Waste  |
| **Whistleblowing records**   | HR  | 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.  | From then outcome date  | Public Interest disclosure Act 1998 and recommended IAPP practice.  |
| **Subject Access Request**   | HR  | 1 year following completion of the request.  | The date of completion of request  | Data Protection Act 2018.  |
| **Insurance Records**   | Finance  | For as long as they are valid  | The date the document was created  | N/A  |
| **Permits, licenses and certificates**   | HR / IT  | For as they are valid, then a maximum of 6 years  | The date issued  | N/A  |
| **Technical and marketing Records**   | Marketing/Service  | Minimum of 10 years  | The date the document was created  | N/A  |
| **Intellectual Property Records**   | Marketing  | Maximum of 6 years after the required period  | The date of registration of the IP  | Section 5 Limitation Act 1980  |
| **Risk assessments including environmental and H&S**   | ISO Manager  | Permanently  | The date the document was created  | management of Health & safety at Work Regulations 1992 S1 1992/2051)  |
| **Debtors and creditors records**   | Finance   | Minimum retention period: these records should be kept for as long as they are relevant to the business operations  | The date the document was created  | N/A  |
| **Customer and Supplier records**   | SOP  | Minimum retention period: these records should be kept for as long as they are relevant up to 6 years  | The date the document was created  | N/A  |
| **Legal /Contracts Records, including Confidentiality and non-competition agreements**   |   | minimum: For the length of the contract or agreement and 6 years afterwards**.**  | The date of execution of the agreement  | Section 5 Limitation Act 1980  |
| **Rental and hire purchase agreements**  | SOP  | Minimum: For the length of the contract or agreement and 6 years afterwards**.**  |   | N/A  |
| **Delivery Notes**   | Warehouse  | Current financial year + 6 years  | Date of note  | VAT Act 1994  |
| **Tendering - Unsuccessful tender documents**  | Finance   | Retain until 1 year after award of contract  | Date of tender  |   |
| **Tendering - Successful tender documents**   | Finance  | Retain until 6 years from end of contract  | Date tender ends  |   |

# Policy Compliance

The Information Security Management Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

# Exceptions

Any exception to the policy must be approved by the policy owner in advance.

# Roles and Responsibilities Implementation of Policy

Failure to comply with this policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Company’s reputation, personal injury, harm, or loss.

Non-compliance with this policy by permanent, temporary or contract employees, or any third parties, who have been granted access to company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

Any suspicion of a breach of this policy must be reported immediately to your Line Manager. All instances of suspected breaches of the policy shall be investigated and action taken as appropriate.