TSL
Crigglestone Industrial Estate
High Street
Crigglestone
Wakefield WF4 3HT

Tel +44 (0)1924 250017
Fax +44 (0)1924 254 964
Email dpo@tslhealthcare.com

www.tslhealthcare.com

Toiletry Sales Group and Subsidiaries (TSL)
Data Retention Policy

TSL recognises that the effective management of its data and records is necessary to comply with its legal and regulatory obligations and contributes positively to the overall management of the business. This document provides the policy framework through which this effective management can be achieved and audited.

Scope of the Policy

- This policy applies to all data records created, received or maintained by staff in the business in the course of carrying out its functions
- Records are defined as all those documents which facilitate the business carried out and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically
- In respect of personal data and sensitive personal data, this policy relates to retention periods which enable us to comply with the requirements of our 'Personal Data Processing Policy' and the requirements of the 'General Data Protection regulations'

Responsibilities

- The business has a corporate responsibility to maintain it's records and record keeping systems in accordance with the regulatory environment and legislative frameworks. The Chief Executive has overall responsibility for this policy.
- The person responsible for records and data management in the business will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved or deleted easily, appropriately and timely.
- In respect of personal data and sensitive personal data processed, the Company has appointed a Data Protection Officer who will ensure compliance with the General Data Protection regulations and report to Board on all related matters.
- Individual employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the business's records management guidelines, data processing policy and data retention policy.

Relationship with Existing Policies

This policy has been drawn up within the context of:

- General Data Protection Regulation (GDPR)
- Freedom of Information Policy
- Other legislation/regulation (including financial, audit, equal opportunities and ethics) affecting the business

Safe Disposal of Records

Where paper records have been identified for destruction they should be disposed of in an appropriate way. All staff records, or sensitive policy information, should be shredded before disposal with a cross cut shredder. All other paper records should be bundled up and disposed of, to a waste paper merchant. Do not put records in the dustbin or a skip.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure records are disposed of in an appropriate way.

Any electronic records that are due to be disposed of in line with this policy, will be deleted permanently and confidentially from all systems when it is appropriate to do so.

Retention Guidelines

Some of the following retention guidelines are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure these retention periods are compliant with the General Data Protection Regulation 2018 and other regulatory requirements. Managing these retention guidelines will be deemed to be 'normal processing' under this legislation.

Data Retention Schedule

Please refer to the **Data Retention Schedule (see Appendix 1)** for more information or specific timescales regarding the retaining of personal data.

In order to classify the data, we have classified the data in terms of its sensitivity within the company.

Sensitivity Level	**Detail**
Secret	Sensitive personal data held in HR or finance in order to be legally complaint. Access to this data is limited to key employees in the department
Confidential	Information specific to a process or person. Access to this data is available to specific key staff, company directors or senior managers.
Internal Only	Information in this area is free to be shared internally but should not be sent externally.
Unrestricted	Data that is free to share

Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will use data efficiently thereby making data management and data retrieval more cost effective. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's management team.

The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden or destroying data in an attempt to cover up a violation of law or company policy.

Department	Type of Data	Sensitivity of Data	Purpose of Data	Retention Period	Comments
HR	HR files and training records, including disciplinary records	Secret	Ensure that all relevant data is retained to meet legal compliance	6 years after employment ceases	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Disciplinary warnings	Secret	Ongoing monitoring of staff performance	Once they have expired in line with disciplinary procedure	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Working Time Records	Secret	Ensure that all relevant data is retained to meet legal compliance	2 years from date made	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Parental Leave	Secret	Ensure that all relevant data is retained to meet legal compliance	5 years after birth / taking of leave	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR/Finance	Wage and Salary records including overtime records and bonuses.	Secret	Ensure that all relevant data is retained to meet legal compliance	7 years	Hard copy printed for initial use but disposed of after use. Long term data stored electronically.
Finance	Payroll and HMRC records	Secret	Ensure that all relevant data is retained to meet legal compliance	7 years	Stored electronically
HR	Right to work in UK	Confidential	Ensure that all relevant data is retained to meet legal compliance	5 years after end of employment	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Medical records/Sick Notes	Secret	Ensure that all relevant data is retained to meet legal compliance	40 years	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Assessments for Health & Safety purposes including accident reports	Secret	Ensure that all relevant data is retained to meet legal compliance	40 years	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
H&S	Health and Safety Reports	Confidential	Monitor of H&S on site	6 Years	Stored electronically
H&S	Health and Safety Records	Confidential	Held for Legal compliance	40 Years	Stored electronically

Department	Type of Data	Sensitivity of Data	Purpose of Data	Retention Period	Comments
Finance	Pension records	Secret	Ensure that all relevant data is retained to meet legal compliance	12 years after benefit ceases	In conjunction with pension provider
HR	Redundancy details and calculations	Confidential	Ensure that all relevant data is retained to meet legal compliance	6 years from date of redundancy	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR	Statutory Mat Pay records calculations and certificates (MATB1)	Confidential	Ensure that all relevant data is retained to meet legal compliance	3 years after the end of the tax year in which maternity period ends	Provided as hard copy, to be scanned into system and original returned to employee
HR / Dept Heads	Appraisals	Confidential	Ongoing evaluation of Staff	6 years after employment ceases	Currently held as Hard Copies. To be transitioned to Electronic copies to ease management of the data
HR / Dept Heads	CV from Prospective Employees	Confidential	Employment of new staff	To be held for a maximum of 1 year after the original application	Held to allow contact / review of prospective employees. To be retained electronically.
HR / Dept Heads	Interview notes	Confidential	Employment of new staff	To be held for a maximum of 1 year after the original application	Held to allow contact / review of prospective employees. To be retained electronically.
HR / Finance	Employee Bank Account Details	Secret	Payment of staff	To be deleted after final pay check.	Provided originally on new starter form. Transferred to electronic system and paper copy destroyed.
All	Electronic Direct contact information	Internal Only	Ongoing working relationships	Maintained for lifetime of Contacts working relationship with TSL	Managed by individual in line with business needs.
All	Business Cards	Internal Only	Ongoing working relationships	Maintained for lifetime of Contacts working relationship with TSL	Hard Copy retained. Managed by individual in line with business needs.
All	Hard copy contact information	Internal Only	Ongoing working relationships	Maintained for lifetime of Contacts working relationship with TSL	Managed by individual in line with business needs.
All	Project Data	Internal Only / Unrestricted	Ongoing working relationships	Lifetime of product and linked products	These are held both as hard copy and electronically. These hold minimal Personal data (mainly contact information) and are

Department	Type of Data	Sensitivity of Data	Purpose of Data	Retention Period	Comments
					retained to ensure that we can work efficiently on future projects
Technical	Panel Test	Confidential / Unrestricted	Evaluation of Products	Final Panel Test are held for lifetime of product. Completed forms are disposed after transfer of data into reports	The original form contains sensitive information. This is anonymised in the final report and original form destroyed.
Technical	Complaints	Confidential	Monitoring of issues	The complaint is logged in a database for trend analysis. The original complaint is stored for the lifetime of the product plus 7 years for legal compliance. Completed health questionnaires are held electronically in folders with limited access	The health questionnaire holds some sensitive information so is scanned and held electronically with the original destroyed once the information has been used.
Technical	External Audit Reports	Confidential	To assess Toiletry Sales and Subsidiaries ability to meet regulatory requirements	10 years	These hold little Personal information but are used for ongoing performance review. Stored electronically.
SLT	Business Continuity Plan	Internal	To allow the business to continue in the eventuality of a serious issue.	Permanently Active	Stored electronically with a paper copy stored securely offsite. There will always be a BCP in place which will be kept live. All previous versions will be destroyed as a new version is implemented.
Technical	Specification	Internal	Details of the product we produce	Lifetime of product and linked products	The old versions of specifications have contact information held in them. This has been removed on new versions but will not be removed on archived documents.
Dept Heads	Management Meeting Minutes	Confidential	Ongoing review of the performance of the business.	5 years	Stored electronically. There is little personal information in the meetings but there may be some discussion around staff issues.

Department	Type of Data	Sensitivity of Data	Purpose of Data	Retention Period	Comments
Warehouse	Drivers Log	Internal	Traceability of product delivered into the warehouse	5 years	Hard copy. Allows control of people into the building but also aids in quarantine in the event of a contagious disease.
HR	Visitor Log	Internal	To control access to the building	1 year	Hard copy. Allows control of people into the building but also aids in quarantine in the event of a contagious disease.