

# Total Laboratory Services Ltd

## Information Retention Policy

### Overview

This Policy details the required retention periods of the personal data Total Laboratory Services Ltd (“we” and/or the “Company”) holds on record and the processes to be applied when destroying that information.

This Policy applies to all business units, processes and systems across all countries where the Company operates.

This Policy applies to all Company staff, agents and contractors who collect, have access to or process personal data on behalf of the Company. It is the responsibility of all of the aforementioned to familiarise themselves with this Policy and ensure compliance with it.

This Policy applies to all information the company collects and uses that pertains to any customer and individual whose data we handle, including, but not limited to the following forms:

- Emails
- Hard Copy Documents
- Soft Copy Documents
- CRM/Database Data
- Video and Audio

This Policy forms part of the company’s Data Protection Policy.

### **1. Retention Rules**

1. For documents not otherwise stated in the Data Retention Schedule, the required period for such data retention will be deemed to be 7 years from the date of creation of the document.
2. The member of staff designated to take responsibility for data protection compliance defines the time period for which the documents and electronic records should be retained. Exemptions to this time period may occur in relation to cases of law suits, court proceedings, criminal investigations and requests by Government bodies.
3. The safeguarding and storage of documents and data will be considered and monitored. All document storage shall be accessible during the retention period by the member of staff designated to take responsibility for data protection compliance, and virtual storage facilities will have a backup procedure to safeguard against technological failure.

4. The Company and its employees will, on a regular basis, review all data held to decide whether to destroy or delete any data once the purpose for which the data was acquired is no longer relevant. Overall responsibility for the destruction of data falls to the member of staff designated to take responsibility for data protection compliance.
5. Data selected for destruction should be deleted, shredded or otherwise destroyed to a degree comparable to its value to others and the confidentiality of its contents. The method of disposal is dependent upon the nature of the document. The Document Disposal Schedule section details the method of disposal. The destruction process may be carried out by an employee or by an external service provider that the Company commissions for this purpose.
6. Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company’s Information Security Policy.
7. Any suspicion of a breach of this policy must be reported immediately to the member of staff designated to take responsibility for data protection compliance and will be fully investigated, and action taken as required.

## 2. Document Disposal

Documents and data selected for disposal shall be destroyed according to the following procedure.

- a) Highly Sensitive – Information that is of a high security value or of a confidential, classified and/or extremely sensitive nature shall be shredded placed in waste collection bins. Virtual data will be permanently deleted and removed from backup files.
- b) Professional - Information that is used for routine business purposes and may contain basic information about a business or individual will be shredded and placed in waste collection bins. Virtual data will be permanently deleted and removed from backup files.
- c) Third-party – Any information unrelated to a specific individual, customer, employee or the business shall be placed in waste disposal bins.

## 3. Data Retention Schedule

Record Category	Retention Period	Record Owner
<b>Finance Records</b>		
Payroll records	Seven years after audit	Finance

Supplier contracts	Seven years after contract is terminated	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance
Financial statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment records (deposits, earnings, withdrawals etc)	7 years	Finance
Invoices	7 years	Finance
Cancelled checks	7 years	Finance
Bank deposit slips	7 years	Finance
Business expenses documents	7 years	Finance
Check registers/books	7 years	Finance
Property/asset inventories	7 years	Finance
Credit card receipts	7 years	Finance
Petty cash receipts/documents	7 years	Finance
<b>Business Records</b>		
Annual corporate filings	Permanent	Finance
Office and team meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Board meeting minutes	Permanent	Finance
<b>Employee Records</b>		
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals etc	As per legal requirement	HR

Applications for jobs, interview notes – Recruitment/promotion panel, where the candidate is unsuccessful	Deleted Immediately	HR
Applications for jobs, interview notes – Recruitment/promotion panel, where the candidate is successful	Duration of employment	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	7 years	HR
Bank details – current	Duration of employment	HR
Payrolls/wages	Duration of employment	HR
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	As per legal requirement	HR
Employee address details	Duration of employment	HR
Expense claims	As per legal requirement	HR
Annual leave records	Duration of employment	HR
Accident books Accident reports and correspondence	As per legal requirement	HR
Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms	As per legal requirement	HR
Pregnancy/childbirth certification	As per legal requirement	HR
Parental leave	Duration of employment	HR
Maternity pay records and calculations	As per legal requirement	HR
Redundancy details, payment calculations, refunds, notifications	As per legal requirement	HR
Training and development records	Duration of employment	HR
<b>Contracts</b>		
Signed	Permanent	Finance

Contract amendments	Permanent	Finance
Successful tender documents and unsuccessful tenders' documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitations	Permanent	Finance
Contractors' reports	Permanent	Finance
Operation and monitoring, eg complaints	Permanent	Finance
<b>Customer Data</b>		
Live chat history	Retained whilst organisation remains a customer. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 6 months.	IT Support
Screen recordings from support sessions	Retained whilst organisation remains a customer. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 6 months	IT Support
TLS Database, CRM and business data – inclusive of Name, job title, email address, telephone/mobile number, address, emails, phone call summaries	Retained whilst organisation remains a customer and/or continuing prospect. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 6 months.	IT Support & Office Manager
Metrics data	Retained whilst organisation remains a customer. Once an organisation requests all records to be deleted, data will be anonymised	IT Support & Office Manager
<b>Non-Customer Data</b>		
Name, email address, job title, address, telephone/mobile number,	Kept until person unsubscribes / requests to be removed from system	IT Support & Office Manager

emails, phone call summaries		
<b>IT</b>		
Recycle Bins	Deleted Monthly	Individual Employee
Downloads	Deleted Monthly	Individual Employee
Inbox, Mail Folders & Deleted Emails	Retained whilst organisation remains a customer and/or continuing prospect. Once an organisation requests all records to be deleted, data will be deleted and removed from back-ups within 6 months. Previous business transactions/records exempt from this.	IT Support & Office Manager
Local PC Drives & files	Reviewed Quarterly – Customer data retained whilst organisation remains a customer. Once an organisation requests all records to be deleted, data will be deleted and removed from the back-ups within 6 months. Previous business transactions/records exempt from this.	Individual Employee
TLS Cloud Server	Reviewed Quarterly - Customer data retained whilst organisation remains a customer. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 6 months. Previous business transactions/records exempt from this.	IT Support & Office Manager

## 4. Policy Management

The owner of this document is the member of staff designated to take responsibility for data protection compliance, who will periodically check, and if necessary, update this document at least once a year.

This document is valid as of: 25/05/2018

**Name:** Sarah Netherway

**Position:** Director and member of staff designated to take responsibility for data protection

**Date:** 21<sup>st</sup> May 2018

**Due for Review by:** May 2019

**Signature:**

A handwritten signature in black ink, appearing to be 'S. Netherway', written in a cursive style.