

Data Retention, Destruction and Disposal Policy



Version number	3.6
Last Approved	Mar 13, 2024
Classification	PUBLIC

Learning Technologies Group plc – Proprietary and Confidential – This document contains confidential information, which is the property of Learning Technologies Group plc, and may not be distributed externally without explicit written permission.

Overview

The Data Retention, Destruction and Disposal Policy defines how long The Company retains data and how it sanitizes, deletes, and disposes of client data and physical hardware used in the hosting of customer data. The policy specifies requirements for data retention, secure destruction and documentation to meet industry best practices and ensure security and privacy for customer data. An overview of how data is backed up is covered by the Data Backup Policy.

Applicability

The applicability of this statement falls under purview of the [Security Documentation Overview](#).

Purpose

This policy defines retention timelines for company and customer data, and the requirements for storing and ensuring data is disposed of in a secure manner. This applies to physical data forms as well as electronic requiring media sanitization.

The reuse, recycling, or disposal of physical electronic devices pose significant risks since data can easily be recovered with readily available tools - even data from files that were deleted long ago or with insecure erasure techniques. Failure to properly purge data in these circumstances may result in unauthorized access to data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

Scope

This policy applies to data stored electronically or in physical form. The level of classification data may receive/be stipulated as only impacts access to that material, and still must comply with these guidelines.

Data Retention

Client Data

Client Data possessed by The Company will be retained for life of service outlined in the contract, and through the export process until customer has acknowledged receipt of data, plus 30 days after termination of service. Data may reside in backups for the duration defined

by [Data Backup Policy](#) .

Log Retention

Logs will be centralized for forensics activity and is subject to our [Data Encryption Policy](#) . Log and metric data will be retained as follows:

1. Application logs: 1 year
2. Security logs (for example all access logs, authorizations, changes, etc.): 3 years

Data Storage

All data shall be stored in a manner that restricts access to authorized personnel executing activities applicable to their role in fulfilling business obligations.

Offline or remote storage of data must be done in a manner that tracks access and prevents accidental data leakage. When possible, third parties utilized in the storage of data shall maintain chain of custody, secure storage with proper physical protections.

Data Destruction & Disposal

Data shall not be retained longer than necessary to adhere to backup and retention policies, inclusive of forensics purposes.

▼ SOC 2: CC6.5

The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Computer systems, electronic devices, and electronic media repurposed or transferred outside of The Company, for any reason, must not contain The Company's data. When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that sensitive and confidential data is rendered unreadable. (e.g., if used computers are disposed of, any sensitive and confidential information that is stored on the machines must be thoroughly erased.)

▼ SOC 2: C1.2

The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Media Destruction (Sanitization Methods)

Media sanitization is conducted by a third-party vendor complying with NIST 800-88 REV 1 and ISO/IEC 27040:2015 standards and requires an accompanying certificate of destruction.

Electronic Storage Media

The following are acceptable methods of sanitizing electronic storage media:

- **Overwriting Magnetic Media** - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization
- **Degaussing** - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state
- **Physical Destruction** – implies complete destruction of media by means of crushing or disassembling the asset.

Paper-Based Media

Paper based media should be shredded or disposed of in secure bins. The Company shall contract with bonded service providers for secure paper media disposal.

3rd Party Sub-processors

Vendors contracts must ensure that any 3rd party sub-processors of Company data are obligated to implement data destruction policies and procedures at least as rigorous as The Company's.

Additional Information

Additional information related to *Disciplinary Actions, Exceptions* and *Questions* can be found in the [Security Documentation Overview](#) .

Document control

i This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 13, 2024
Review cycle	ANNUAL	
Next review date	Mar 13, 2025	

Version History

Date	Author(s)	Version	Changes
Oct 28, 2024	@Art Machado @Paul Gordon @angelina.kilmer	3.6	Log retention updates. Changed Policy classification from Confidential to Public.-
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	3.5	Annual review
Feb 23, 2023	@Art Machado , @Sarah Zwicker (Unlicensed)	3.4	Annual review + logo updated
Apr 14, 2022	@Sarah Zwicker (Unlicensed)	3.3	Added reference to Data Backup Policy.
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	3.2	Added Privacy considerations and components
Mar 16, 2022	@Art Machado , @Sarah Zwicker	3.1	Title change for VP InfoSec, Annual Policy review

	(Unlicensed)		
Nov 18, 2021	@Art Machado & @Jaimie Livingston	3.0	Added Data Retention
May 20, 2021	@Art Machado	2.9	Added Sub-processor clause
Mar 11, 2021	@Sarah Zwicker (Unlicensed)	2.8	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.7	Reformatted, policies linked
Jan 26, 2021	@John Cole	2.6	Annual review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.5	Changed owner