DATA RETENTION POLICY

1. PURPOSE

The purpose of this policy is to establish a clear framework for the retention, review, and disposal of personal and commercial data processed by DSW. The policy ensures compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant legal and contractual obligations. It aims to promote effective data management, reduce risks associated with unnecessary data retention, and safeguard both individual privacy and commercial confidentiality.

2. SCOPE

This policy applies to all personal and commercial data collected, stored, or processed by DSW, whether in electronic or physical format. It applies to:

- All employees, contractors, and third-party service providers acting on behalf of DSW
- All data processing activities, including collection, storage, access, sharing, and deletion
- All business areas and departments within DSW

Data covered by this policy includes:

- Personal data of employees, clients, learners, suppliers, and consultants
- Commercial data such as contracts, invoices, policies, and project documentation

3. DEFINITIONS

Personal Data: Any information relating to an identifiable individual, as defined by the UK GDPR.

Special Category Data: Sensitive personal data that requires additional protection under data protection law.

Commercial Data: Non-personal data relating to business operations, including contracts, business contacts, supplier and client information, financial records, and internal documents.

Data Subject: An individual whose personal data is processed by DSW.

Data Retention: The practice of storing data for a defined period for legal, operational, or regulatory reasons, after which the data should be securely disposed of.

4. POLICY STATEMENT

DSW is committed to managing personal and commercial data responsibly and in compliance with UK GDPR and other relevant legal requirements. Data shall not be retained longer than necessary for its intended purpose. This policy ensures that:

- Retention periods are defined, justified, and regularly reviewed
- Data subjects' rights under UK GDPR are upheld
- Commercial data is handled securely and in line with confidentiality obligations
- Disposal of data is undertaken in a secure and consistent manner

DSW shall maintain clear procedures to regularly review and securely dispose of data no longer required, while allowing for legal, contractual, or regulatory exceptions where applicable.

5. PROCEDURES

5.1 DATA COLLECTION AND CLASSIFICATION

Data collected by DSW shall be identified and classified as personal or commercial. The classification determines the appropriate retention period, as defined in Appendix A.

5.2 STORAGE AND ACCESS

All data shall be stored securely:

- Digital data: on encrypted, access-controlled systems hosted either on company premises or approved third-party platforms
- Physical data: in locked cabinets or restricted areas within company premises
- Access shall be limited to authorised personnel only.

5.3 RETENTION PERIODS

Retention periods are defined according to legal, regulatory, or operational requirements. Where no statutory period applies, data shall be retained for no longer than necessary for the original purpose.

Retention periods are detailed in Appendix A and subject to annual review.

5.4 DATA REVIEW

An annual review of all data holdings shall be conducted to ensure:

- Data is accurate, up to date, and still required
- Retention periods are being respected
- Data identified for disposal is flagged for secure deletion

5.5 DATA DISPOSAL

Upon reaching the end of its retention period or when no longer required:

- Digital data shall be securely deleted using permanent erasure tools
- Physical data shall be destroyed using cross-cut shredding or confidential waste disposal services

6. ROLES AND RESPONSIBILITIES

Compliance Manager

- Oversees the implementation and compliance of this Policy.
- Monitors legal and regulatory updates.

Heads of Department

- Implement the Policy locally.
- Maintain departmental risk assessments.

All Users

- Follow data retention policies and procedures.
- Report actual or suspected breaches immediately.

7. MONITORING AND REVIEW

- All staff will undergo annual training related to Data Protection, Retention and Information Security.
- This policy will be reviewed biannually by the Governance Team to ensure it remains current and effective.
- Compliance with this policy will be audited as part of the ISO9001 Quality Management System.

8. RELATED POLICIES AND DOCUMENTS

Other policies and procedures that relate to this document. Examples:

- DSW Data Protection Policy (UK GDPR)
- DSW Information Security Policy

9. REGULATORY REFERENCES

This Policy is aligned with:

- UK GDPR

10. CONTACT INFORMATION

For further information or clarification, contact:

- Hayley Morgan, Compliance Manager – hmorgan@dswlearning.co.uk
- Hayley Doran, Head of Operations – hdoran@dswlearning.co.uk

APPENDIX A: DATA RETENTION SCHEDULE

Type of Data	Description	Purpose	Review Period	Retention Period or Criteria
Consultant Details	Contact details, CV, ID, company and VAT numbers	Payments, employment facilitation	Annually	Duration of contract or upon request for removal
Apprentice Details	Unique learner number, employer, training provider, assessment data	Conducting endpoint assessments	Annually	Six years
Employee Details	Employment, financial, and HR records	Employment processing and HMRC compliance	Annually	Six years after employment ends
Delegate Details	Name, email	Course registration and communication	Annually	Duration of course or client contract
Client Details	Contact info, contracts, billing records	Communication, invoicing, legal compliance	Annually	Six years after contract ends
Supplier Details	Business contacts, contracts, billing info	Communications and payments	Annually	Duration of contract or upon request for removal
Commercial Contracts and Agreements	Supplier, partner, client contracts	Contractual and legal obligations	Annually	Six years or longer where legally required
Internal Operational Records	Policies, project files, strategic documents	Internal operations and auditing	Annually	Reviewed periodically; up to ten years or as necessary