DeGesh School of Entrepreneurship

Data Retention Policy

Policy Review Date	30/01/2025
Next Review Date	29/01/2026

1. Purpose

This policy helps to ensure that the DeGesh School of Entrepreneurship (DSE) appropriately manages and retains its data in compliance with legal, regulatory and business requirements. This policy sets the guidelines for data preservation, safe storage, and deletion of unnecessary data.

2. Scope

This policy is for all information produced, received or maintained by DSE including but not limited to student records, employee data and financial documents as well various correspondence. It includes data in electronic and physical form.

3. Data Retention Periods

The period of time for which data is to be retained will depend upon its nature, as well as regulatory or other requirements and/or School operational needs. Below are the general retention years for important types of data:

- Student Records (portfolios and assessments): Stored until certification is issued, then will be permanently deleted within 14 days.
- Student ID and Educational Documentation: Retained for 1 year and then permanently deleted.
- Student Certificate: Not stored as certificates are downloadable from awarding body portal.
- Records of Financial: Kept for at least 7 years to meet standards in accounting practices and tax laws.
- Records of Employment: Support documents 1 years after the employee leaves employment
- Contractual Agreement: All records are retained for the duration of employment an 90 days following termination of employment.
- Emails and Correspondence: Saved for at least one year with relevant emails filed away or deleted.
- Onboarding Documents: Keep for the duration of the learner's enrolment plus 1 years after their course completion or withdrawal.

4. Data Archiving

Data which needs to be retained past its operational use, the data will be securely archived for the desired retention period. For compliance and audit purposes, all archived data must be secure from unauthorized alteration or deletion during the expected retention period. Only authorised staff will be allowed to access the archived data.

5. Data Disposal

Data beyond its retention period should be securely disposed to avoid unauthorised access or data leakages. Disposal methods include:

- Digital Data: Erase permanently from servers, databases and backup system.

- Physical Documents: All physical data beyond the retention period are securely shredded are disposed of.

6. Data Protection and Security

DSE is dedicated to safeguarding the confidentiality, integrity and availability of data in every stage of its lifecycle. Adequate technical and organisational measures shall be implemented in order to protect Personal Data from unauthorised access, accidental loss or destruction.

7. Regulatory and Legal Compliance

This policy is applicable to the protection of human subjects and data, assures compliance with all relevant GDPR laws and regulations. We may also change the retention periods based on changes in our legal obligations or practice standards.

8. Responsibilities

- Data owners decides the type and period of data that needs to be retained, archived, or disposed of.
- · The IT team maintains technical infrastructures supporting data retention, arcing. Imposing proper disposal practices
- · Compliance team monitors the legal/regulatory environment to detect changes which may have an impact on data retention.

9. Policy Review

This Data Retention Policy must be reviewed on an annual basis or as requested to ensure that it is current due to legal, regulatory and business requirements.

10. Exceptions

All exceptions to this policy must be approved by the governing board and documented as such.

11. Enforcement

Failure to comply may result in discipline, up to and including termination of employment or contracts.