Data Protection Policy

Version 1.0 | Date: March 2025

Applies to: All Students, Staff, and External Partners of Advanced Learning

Purpose and Scope

This policy ensures that Advanced Learning complies with the General Data Protection Regulation (GDPR) and Maltese data protection laws by outlining how personal data is collected, processed, stored, and shared. It applies to all students, staff, contractors, and third parties involved in data processing, across both physical and digital formats.

Definitions

Personal data refers to any information identifying a person, such as names or contact details. Processing includes collecting, storing, and using data. The data subject is the individual to whom the data belongs. Advanced Learning acts as the data controller, while any external entity handling data on its behalf is considered a data processor.

Principles of Data Protection

Advanced Learning processes data lawfully, fairly, and transparently, for clear and legitimate purposes. Only necessary and accurate data is collected, stored securely, and retained no longer than required. The institution accepts full accountability for upholding these principles.

Types of Data Collected

We collect student, staff, and third-party data, including contact information, academic records, financial details, and system activity logs. Sensitive data, such as medical or demographic information, is only processed with explicit consent or legal justification.

Legal Basis for Processing

Data is processed on the basis of consent, contract performance, legal obligation, vital interest, or legitimate institutional interest, provided that individual rights are not overridden.

Individual Rights

Data subjects have the right to access, correct, delete, or restrict their data, object to its use, request data portability, withdraw consent, and lodge complaints with the IDPC. Requests may be submitted via [Insert Email].

Data Sharing and Transfers

Personal data is shared internally and with approved processors under strict agreements. No data is transferred outside the EU without appropriate safeguards.

Security and Breach Response

We use encryption, secure passwords, limited access, and regular backups to protect data. Breaches must be reported to the Data Protection Officer immediately and may be escalated to the IDPC within 72 hours.

Records and Retention

We maintain a processing register outlining data types, purposes, legal bases, and retention periods. Academic records are retained for 10 years, assessment records for 5, financial records for 7, and admissions data for up to 1 year post-course unless required longer.

Version: 1.0
Effective Date: March 2025 **Next Review Date:** March 2026

Review

This policy is reviewed annually by the Data Protection Officer to ensure continued compliance with evolving data protection regulations.