Data Management Policy

Aspect of QA	Data Protection and Information Management
Policy Owner	Managing Director / Data Protection Lead
Purpose	To outline how Swan ELT collects, processes, stores and protects personal data in compliance with GDPR.
Scope	This policy applies to all staff, students and third parties whose personal data may be processed by Swan ELT.
Related Policies	Data Management Policy, IT Security Policy, Student Records Policy
Review Cycle	Annual

School Name: Swan Training Institute
Address: 11 Grafton Street, Dublin 2, Ireland, D02 H599
CRO Number: 138208
Data Protection Lead (DPL): Helen Gao

1. Introduction

Swan Training Institute is committed to protecting the personal data of our students, staff, agents, host families, partners and visitors.

This policy explains:

- What personal data we collect
- Why we collect it
- How we protect it
- How long we keep it

- Your rights under GDPR

We comply with:

- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- The Irish Data Protection Act 2018

This policy applies to all staff, contractors and anyone processing personal data on behalf of Swan Training Institute.

2. Key Principles

We follow the 7 GDPR principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

3. Who Is Responsible

Data Controller: Swan Training Institute
Data Protection Lead (DPL): Helen Gao (Administration Manager)

The DPL is responsible for:

- Monitoring GDPR compliance
- Handling data breaches
- Managing subject access requests
- Ensuring staff training
- Reporting serious breaches to the Data Protection Commission

All staff are responsible for protecting personal data in their daily work.

4. What Personal Data We Collect

We may collect:

Students;

- Name, date of birth, nationality
- Passport details
- Contact details
- Emergency contact information
- Payment details
- Academic records
- Attendance records
- Visa documentation (where relevant)
- Medical or dietary information (where necessary)

Staff:

- Contact details
- PPS number
- Bank details
- Employment records
- Garda Vetting results (where required)
- Health information (limited and lawful)
- CCTV Data
- Video recordings of individuals on our premises

5. Lawful Basis for Processing

We process data based on:

- Contract (student enrolment / employment contract)
- Legal obligation (Revenue, Garda Vetting, safeguarding)
- Legitimate interest (school administration, safety)
- Consent (marketing, photos, certain medical disclosures)
- Special category data (e.g., health information) is processed only when legally permitted.

6. CCTV Policy

Swan Training Institute uses CCTV for:

- Security of students and staff
- Crime prevention
- Health and safety monitoring
- Protection of school property
- CCTV Controls

1. Clear signage is displayed at entrances
2. Cameras are positioned for security purposes only
3. Recordings are stored securely
4. Access is restricted to authorised personnel only
5. Footage is normally retained for 30 days unless required for investigation
6. CCTV footage may be shared with An Garda Síochána where legally required.

Individuals may request access to CCTV footage of themselves through a Subject Access Request.

7. Data Retention Schedule

Data is securely destroyed after retention periods expire.

8. Data Security Measures

We protect data by:

- Password-protected systems
- Role-based access controls
- Secure cloud storage
- Encrypted devices
- Locked filing cabinets
- Regular data backups
- Staff training

Staff must:

- Not share passwords
- Avoid sending sensitive data by unsecured email
- Report suspected breaches immediately

9. Data Breach Procedure

A data breach includes:

- Sending personal data to the wrong person
- Loss of a laptop or USB device
- Hacking or malware attack
- Loss of files

If a breach occurs:

- Inform the Director immediately.
- The breach will be assessed.
- If required, the Data Protection Commission will be notified within 72 hours.
- Affected individuals will be informed if risk is high.
- All breaches are recorded in a Data Breach Log.

10. Sharing Personal Data

We may share data with:

- Revenue Commissioners
- An Garda Síochána
- Data Protection Commission
- Visa authorities
- Payment processors
- IT service providers
- Insurers
- Professional advisers

We ensure data processing agreements are in place where required.

We do not sell personal data.

11. Transfers Outside the EEA

If personal data is transferred outside the European Economic Area, we ensure appropriate safeguards such as Standard Contractual Clauses are in place.

12. Garda Vetting

All relevant staff working with minors are Garda vetted in accordance with Irish law.

Vetting disclosures are:

- Stored securely
- Access restricted
- Not shared unlawfully
- Deleted after the retention period

13. Your Rights

Under GDPR, individuals have the right to:

- Access their data
- Rectify inaccurate data
- Erase data (in certain cases)
- Restrict processing
- Object to processing
- Data portability
- Lodge a complaint with the Data Protection Commission

Requests must be made in writing to the DLA.

We respond within one month.

14. Subject Access Requests (SAR)

To make a request:

- Submit request in writing
- Provide proof of identity

We will:

- Confirm receipt
- Assess the request
- Provide data securely

We may refuse requests that are excessive or unfounded as permitted by law.

15. Staff Training

All staff receive GDPR training:

- On induction
- When policies change
- Periodically as refresher training
- Attendance is recorded.

16. Monitoring and Review

This policy is reviewed annually by the DLA.

Last Updated: March 2026

17. Contact Details

Swan Training Institute
11 Grafton Street
Dublin 2
D02 H599
Ireland

Data Protection Lead (DPL): Helen Gao
Email: admin@selt.ie
Phone: +353 1 6775252

Data Protection Responsibilities Overview

Area	Responsible Person	Action
Data Collection	Administrative Staff	Ensure data is collected lawfully and for specified purposes.
Data Storage	IT / Administration	Store personal data securely and limit access.
Data Protection Compliance	Management / Data Protection Lead	Monitor compliance with GDPR requirements.