

Academic Bridge Data Management Policy

Version: 2.0 (Reorganized for Enhanced Clarity and Completeness)

Date: 16/03/2026

Approved by: Senior Management Committee (SMC)

Data Protection Officer:

Mark Anthony (mark.anthony@academicbridge.ie | Phone: +353-894425810)

Review Frequency: Annually or upon legislative changes.

Table of Contents

1. Introduction & Definitions	2
2. Purpose & Commitment	2
3. Scope of Application	2
4. Data Protection Principles	3
5. Types of Personal Data Processed	3
6. Governance and Accountability	4
7. Lawful Basis for Processing & Consent Management	4
8. Data Subject Rights & How to Exercise Them	5
9. Security of Personal Data	5
10. Data Sharing & Third Parties	6
11. International Transfers	6
12. Personal Data Breach Management	6
13. Privacy Notices & Transparency	6
14. Contact Information & Complaints	6
15. Monitoring & Review	7
Appendices	8
A: Data Retention Schedules	8
B: Data Protection Impact Assessment (DPIA) Template	9
C: Subject Access Request (SAR) Form	9
D: Consent Form Templates	10

1. Introduction & Definitions

This policy ensures Academic Bridge (AB) complies with the General Data Protection Regulation (GDPR) and the Irish Data Protection Acts 1988-2018. It promotes a culture of privacy by design and accountability.

Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person (e.g., name, email, ID number, location data).
- **Data Subject:** The individual whose personal data is processed (e.g., students, staff, visitors).
- **Data Controller:** AB, responsible for determining the purposes and means of processing personal data.
- **Data Processor:** Third parties (e.g., cloud providers) acting on AB's instructions to process personal data.
- **Processing:** Any operation on personal data, including collection, storage, use, or deletion.
- **Special Category (Sensitive) Data:** Data revealing racial/ethnic origin, political opinions, religious beliefs, health, biometric data, or criminal convictions.
- **Record of Processing Activities (ROPA):** A documented inventory of all data processing activities.
- **Data Protection Impact Assessment (DPIA):** An assessment for high-risk processing to identify and mitigate privacy risks.

2. Purpose & Commitment

Academic Bridge (AB) is fully dedicated to ensuring the confidentiality, integrity, and security of personal data belonging to students, faculty, staff, and stakeholders. This policy defines our structured procedures for the collection, handling, and storage of information in strict accordance with the GDPR and the Irish Data Protection Acts. We recognise that privacy is a critical pillar of an academic environment and strive to foster a culture of accountability and transparency, ensuring that data is managed ethically to maintain the trust and confidence of our college community.

3. Scope of Application

This policy is institution-wide and applies to:

- Personnel: All staff, contractors, and service providers with access to IT systems.
- Data Types: All personal data regarding learners, employees, and third-party stakeholders (such as agents) in both physical (paper) and digital formats.
- Infrastructure: All cloud-hosted platforms (email, file storage, finance tools), physical hardware (laptops, mobile devices), and on-site storage facilities.

4. Data Protection Principles

Academic Bridge adheres to the core principles of the GDPR to ensure data is managed responsibly:

- Lawfulness, Fairness, and Transparency: Data is processed legally and individuals are clearly informed of how their data is used.
- Purpose Limitation: Information is collected for specified, legitimate academic or administrative goals and not repurposed without a legal basis.
- Data Minimisation: Only the minimum necessary data required for a specific purpose is collected and processed.
- Accuracy: We take reasonable steps to ensure data is accurate and kept up to date.
- Storage Limitation: Data is retained only for the duration of the study plus three years (for learners) or as required by law, then securely destroyed or anonymized.
- Integrity and Confidentiality: Appropriate technical and organisational measures are used to prevent unauthorised access or accidental loss.
- Accountability: As a Data Controller, Academic Bridge must demonstrate compliance with these principles at all levels.

5. Types of Personal Data Processed

AB processes various categories of personal data, always applying data minimisation:

- Student Data: Academic records, enrolment details, financial information, Garda vetting results, disciplinary records.
- Staff Data: Employment contracts, payroll, performance reviews, health, and safety records.
- Visitor/Third-Party Data: Contact details for agents, accreditation bodies, or medical insurers.

- Sensitive Data: Health information (e.g., for accessibility needs), immigration status for international students, or criminal records (via vetting).

All processing is logged in the ROPA.

6. Governance and Accountability

- Data Protection Officer (DPO): Mark Anthony oversees policy implementation, conducts audits, manages Data Access Requests (DAR), and liaises with the Data Protection Commission (DPC).
- Record of Processing Activities (ROPA): Maintained by the DPO as an inventory of data processing.
- Data Protection Impact Assessments (DPIA): Conducted for high-risk activities (e.g., new technologies or large-scale sensitive data processing).
- Staff Training: Mandatory annual GDPR training for all relevant staff, integrated into inductions.
- Bi-Annual Compliance Sign-Off: Departmental leads review and sign off on compliance every six months.

7. Lawful Basis for Processing & Consent Management

We process data under the following legal grounds:

- Contractual Necessity: For staff/learner contracts (e.g., payroll, course delivery).
- Legal Obligation: For tax, immigration (GNIB/INIS), or accreditation (QQI) requirements.
- Vital Interests: For health/safety emergencies.
- Legitimate Interests: For promotion/communication, balanced against individual rights.
- Consent: For non-essential activities (e.g., marketing). Sensitive data requires explicit written consent.

Consent Procedures

- Obtained via clear, informed forms (see Appendix D).
- Easily withdrawable at any time via email to DPO.
- For minors (under 18), consent from parents/guardians is required.
- Records of consent maintained for audit purposes.

8. Data Subject Rights & How to Exercise Them

Individuals have robust rights:

- Right of Access: Submit a SAR (see Appendix C) to receive data copies within one month (extendable to two).
- Right to Rectification: Correct inaccurate data.
- Right to Erasure ("Right to be Forgotten"): Delete unnecessary data.
- Right to Portability: Receive data in structured format.
- Right to Object/Restrict: Stop processing for certain purposes.
- Right to Object to Automated Decisions: Challenge profiling.

Requests are free unless manifestly unfounded/repetitive. Appeals go to the DPO.

9. Security of Personal Data

Academic Bridge ensures the security of personal data through appropriate technical and organisational measures in line with GDPR requirements. Personal data, including learner records, assessment results, attendance, and staff information, is managed through an integrated ERP (Enterprise Resource Planning) system, which supports core school operations such as.

- a. student enrolment,
- b. attendance and progress tracking,
- c. timetabling,
- d. class allocation,
- e. fees and finance management,
- f. staff records, and reporting.

This data is securely stored on AWS (Amazon Web Services) cloud infrastructure using a MySQL database. Access is controlled through password protection and role-based permissions, ensuring that only authorised personnel can access information on a need-to-know basis.

Physical records are maintained in locked storage areas with restricted access. Staff are trained in data protection and are required to manage data confidentially at all times. Secure procedures are followed when sharing data with relevant bodies such as

accreditation and immigration authorities, and all data is regularly backed up and monitored. Any data breaches are reported and managed promptly in accordance with established procedures.

10. Data Sharing & Third Parties

Data shared only when necessary (e.g., with accreditation bodies, insurers). All processors sign Data Processing Agreements ensuring GDPR compliance. No sharing without legal basis.

11. International Transfers

Transfers outside EU/EEA prohibited unless safeguards apply (e.g., Standard Contractual Clauses or adequacy decisions). For international students, data shared with INIS under legal obligations.

12. Personal Data Breach Management

A breach compromises data confidentiality/integrity/availability.

- Notification: Report immediately to DPO/CEO.
- Reporting: Notify DPC and affected individuals within 24 hours.
- Remediation: SMC conducts root-cause analysis and updates policies.

13. Privacy Notices & Transparency

Separate privacy notices provided to students, staff, and visitors at collection points (e.g., enrolment forms, websites). Notices detail processing purposes, legal basis, rights, and contacts. Updated annually and accessible on AB's website.

14. Contact Information & Complaints

- DPO: Mark Anthony, mark.anthony@academicbridge.ie, +353894425810.
- SAR/Complaints: Submit to DPO; processed within one month.
- Supervisory Authority: Data Protection Commission (DPC), Canal House, Station Road, Portarlinton, Co. Laois. R32 AP23. Tel: +353 57 868 4800 | Email: info@dataprotection.ie | Website: www.dataprotection.ie.
- Individuals may complain to DPC if unsatisfied with AB's response.

15. Monitoring & Review

Reviewed annually or upon changes. Internal audits ensure compliance. Version control maintained below:

Version	Date	Changes Made	Approved By
1.0	02/03/2025	Initial policy	OMB
2.0	19/03/2026	Reorganization & enhancements	SMC

Appendix A: Data Retention Schedules

HR Records

Record	Retention Period	Disposal Method
Health & safety consultations	Duration of contract + 3 years	Archiving
Disciplinary/training records	3 years after employment ceases	Secure deletion
Payroll records	3 years after tax year	Secure deletion
Application forms (unsuccessful)	1 year	Secure deletion
Senior executives' records	Permanent	Archiving

Learner & Academic Records

Record	Retention Period	Disposal Method
Student enrolment records	Duration of studies + 3 years	Secure deletion

Module grades/transcripts	Duration of course + 3 years	Archiving
Garda vetting records	Duration of studies + 1 year	Secure deletion
Discipline records	Duration of studies + 7 years	Secure deletion
QQI/ACELS Reports	Permanent	Archiving
Assessment scripts (unreturned)	1-month post-appeal deadline	Secure deletion

Appendix B: Data Protection Impact Assessment (DPIA) Template

1. Description of Processing: [Outline activity, e.g., new student app].
2. Necessity & Proportionality: [Legal basis, data minimised?].
3. Risks to Rights/Freedoms: [High/medium/low; impacts on data subjects].
4. Mitigation Measures: [Technical/organisational controls].
5. Consultation: [With DPO/stakeholders].
6. Approval: [Signed by DPO/SMC].

Appendix C: Subject Access Request (SAR) Form

Requester Details: Name, Contact, Relationship to AB.

Request Details: What data? Purpose?

Declaration: I confirm this is my request.

Submit to: DPO@academicbridge.ie.

AB will respond within 1 month.

Appendix D: Consent Form Templates

General Consent Form

I, [Name], consent to AB processing my [data type] for [purpose]. I understand I can withdraw consent anytime.

Signature: _____ Date: _____

Marketing Consent

I consent to receiving updates from AB via [email/post]. Opt-out anytime.

Signature: _____ Date: _____