

Data Protection Policy

1. Introduction

Academic Bridge is fully dedicated to ensuring the confidentiality and security of personal data belonging to our students, staff, and other stakeholders. This Data Protection Policy defines our procedures for the collection, handling, storage, and distribution of personal information, in accordance with relevant data protection regulations and best practices. We recognize the critical importance of preserving privacy and safeguarding information within an academic environment. We strive to prevent unauthorized access, misuse, or exposure of sensitive information while upholding the integrity of our educational and administrative operations. Academic Bridge collects personal information from both employees and students through a variety of channels and takes full responsibility for the security of this data. The roles and responsibilities related to data protection for students, educators, and instructors are outlined in both the teacher/instructor and student handbooks.

2. Purpose

This Data Protection Policy is designed to assist the college in fulfilling its obligations concerning the handling of personal data and complying with legal requirements under applicable data protection laws. Additionally, the policy improves transparency by specifying how Academic Bridge expects personal data to be managed. It also provides a detailed explanation of the type of data collected, the reasons for its collection, the duration of storage, and the circumstances under which it may be shared.

By following this policy, AB aims to maintain the highest standards of data security while building trust and confidence within the college community.

The following are the key goals of this Data Protection Policy:

- To safeguard the rights and privacy of individuals by ensuring their personal data is handled securely and ethically.
- To foster a culture of awareness and accountability regarding data protection throughout the college community.
- To set up clear protocols for managing data breaches, ensuring prompt actions to minimize potential risks.
- To outline the roles and duties of staff and students in handling personal data in accordance with legal and institutional standards.
- To ensure that data is used solely for valid academic, administrative, or operational purposes, preventing unauthorized access or misuse.

3. Types of Personal Data Collected

Academic Bridge collects and processes the following types of personal data:

Students: Name, date of birth, address, contact details (phone, email), nationality, academic qualifications, payment information, and attendance records.

Staff: Name, contact details, employment history, salary information, and any other necessary information related to employment.

Other Stakeholders: Contact information for agents, and other associated individuals.

4. Legal Basis for Processing Data

Personal data will be processed on the following legal bases:

Consent: Where individuals have provided explicit consent.

Contractual Necessity: To fulfil our contractual obligations with students and staff.

Legal Obligation: Where processing is necessary to comply with legal or regulatory requirements.

Legitimate Interests: To protect the interests of the school, staff, and students.

5. Data Retention

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Once the data is no longer required for the purpose it was collected, it will be securely deleted or anonymized in accordance with legal retention periods.

6. Data Security Measures

We take appropriate technical and organizational measures to ensure the security of personal data, including:

• **Secure storage of physical and digital records.**

Access controls and role-based permissions to restrict access to personal data.

Regular staff training on data protection and security.

7. Sharing of Personal Data

Personal data will not be shared with third parties, except where required to do so by law or to fulfil

contractual obligations (e.g., sharing data with educational bodies, accreditation agencies, or

payment processors). Where data sharing with third parties is necessary, the third parties will be

required to comply with the data protection requirements set forth in this policy.

8. Data Breach Notification

In the event of a data breach, Academic Bridge will promptly notify affected individuals and the Data Protection Commissioner within 24 hours of becoming aware of the breach.

9. Employee and Student Responsibilities

All staff, students, and contractors are required to:

Handle personal data with care and confidentiality.

Follow the procedures set out in this policy and any additional guidance provided by the school.

Immediately report any security incidents, breaches, or concerns regarding data protection

to the Data Protection Officer.

10. Review of Policy

This Data Protection Policy will be reviewed regularly to ensure ongoing compliance with data

protection laws and to improve our practices. Any updates will be communicated to staff and

students as necessary.