GDPR PRIVACY POLICY *(Website + Internal Compliance Policy)*

1. Introduction

1.1 This GDPR Privacy Policy establishes the Organisation's internal and external standards for the lawful, fair, and transparent processing of Personal Data. It complements the Privacy Notice and applies to all staff, contractors, and systems involved in collecting or processing Personal Data.

1.2 The purpose of this Policy is to ensure compliance with the UK GDPR, the DPA 2018, the Privacy and Electronic Communications Regulations (PECR), and relevant guidance issued by the Information Commissioner's Office (ICO).

1.3 This Policy applies to all Personal Data processed through the Organisation's website, CRM systems, email accounts, application platforms, and internal records.

2. Scope

2.1 This Policy applies to all business areas and personnel, including:

- recruitment counsellors;
- admissions and visa support teams;
- marketing staff;
- partner relationship managers;
- administrative staff;
- contractors and third-party service providers.

2.2 All information systems that process Personal Data, whether cloud-based or on-premises, fall within the scope of this Policy.

3. Data Protection Principles

The Organisation adheres to the six principles of data protection under Article 5(1) UK GDPR:

3.1 **Lawfulness, Fairness, Transparency**
Personal Data is processed lawfully, fairly, and transparently.

3.2 **Purpose Limitation**
Data is collected for explicit and legitimate purposes and not further processed for incompatible purposes.

3.3 **Data Minimisation**
Only data strictly necessary for operational purposes is collected.

3.4 **Accuracy**
Information must be accurate and kept up to date.

3.5 **Storage Limitation**
Data is retained only for as long as necessary.

3.6 **Integrity and Confidentiality**
Data is processed securely using appropriate safeguards.

3.7 **Accountability**
The Organisation demonstrates compliance with all principles.

4. Lawful Processing

4.1 All processing activities must be supported by a valid lawful basis under Article 6 UK GDPR.

4.2 Staff must confirm the lawful basis before collecting or processing Personal Data and must not rely on consent where another basis is more appropriate.

4.3 Special Category Data requires an Article 9 condition and additional safeguards.

5. Privacy by Design and Default

5.1 The Organisation integrates privacy considerations into all stages of system and service design.

5.2 New projects involving Personal Data require a Data Protection Impact Assessment (DPIA) if they present a high risk to individuals.

5.3 Default settings must ensure that only Personal Data necessary for each purpose is processed.

6. Website Data Collection

6.1The following Personal Data may be collected via the Organisation's website:

- enquiry form submissions;
- application uploads;
- cookie-generated analytics;
- IP addresses and device information;
- communication preferences.

6.2 All website forms must include a privacy information statement and, where needed, an explicit consent request.

7. Use of Cookies and Tracking Technologies

7.1 The Organisation uses essential cookies for core website functionality.

7.2 Analytics and marketing cookies require user consent under PECR.

7.3 Users must be provided with a cookie banner and a clear opt-in/opt-out mechanism.

8. Marketing and Communications

8.1 Marketing activities must rely on either consent or legitimate interests.

8.2 Unsubscribe/opt-out instructions must be included in all electronic communications.

8.3 Marketing lists must be regularly cleansed to remove unsubscribed individuals.

9. Contracts with Third Parties

9.1 Third-party suppliers processing Personal Data must sign a Data Processing Agreement meeting Article 28 UK GDPR requirements.

9.2 Due diligence must be conducted before engaging any Processor, and reassessed periodically.

9.3 Third parties cannot use or disclose Personal Data for their own purposes.

10. Data Subject Requests

10.1 All staff must recognise Data Subject access or rights requests and direct them immediately to the data protection contact point.

10.2 Requests must be responded to within statutory deadlines.

11. International Data Transfers

11.1 Transfers outside the UK must use an approved lawful mechanism, including:

- adequacy regulations;
- Standard Contractual Clauses (SCCs);
- explicit consent; or
- legally recognised safeguards.

11.2 Transfer risk assessments must be conducted as necessary.

12. Data Retention

12.1 Retention periods must be followed as outlined in the Data Retention & Deletion Policy.

12.2 Staff must ensure that outdated data is securely deleted or anonymised.

13. Information Security Responsibilities

13.1 Staff must protect all Personal Data they access and follow internal security procedures.

13.2 Common obligations include:

- password protection;
- safeguarding devices;
- avoiding unauthorised disclosure;
- reporting incidents or near-misses immediately.

14. Monitoring and Audit

14.1 The Organisation conducts periodic reviews of compliance with this Policy.

14.2 Non-compliance may result in disciplinary action.

15. Roles and Responsibilities

15.1 The Data Protection Officer or Privacy Lead oversees compliance.

15.2 All staff share responsibility for protecting Personal Data.