Data Protection Policy

1. Purpose

This policy sets out how Nisai Group Limited and its subsidiaries ("the Company") comply with the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 in collecting, using, storing, and disposing of personal data.

2. Definitions

- Company: Nisai Group Limited and all associated subsidiary companies
- Personal Data: Any information relating to an identified or identifiable individual
- Processing: Any operation performed on personal data, including collection, storage, use, or deletion
- Data Subject: An individual whose data is processed
- DPO: Data Protection Officer – Dai Patel (dai.patel@nisai.com | 020 8424 8475)
- Register of Systems: Internal register of all systems and processes where personal data is held or processed

3. Data Protection Principles

The Company commits to processing data in line with Article 5 of the GDPR. Personal data must be:

1. Lawfully, fairly and transparently processed
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed securely, protecting against unauthorised access, loss or destruction

4. Responsibilities

- The DPO is responsible for overseeing GDPR compliance and reviewing this policy annually
- All staff handling personal data must comply with this policy and receive appropriate training

5. Lawful Bases for Processing

The Company ensures that all personal data is processed under a recognised lawful basis, including:

- Consent (with clear opt-in and withdrawal)
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Each processing activity is recorded in the Register of Systems, along with its lawful basis.

6. Rights of the Individual

The Company recognises and upholds the following rights of data subjects:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making

Requests must be acknowledged promptly and fulfilled within one calendar month where applicable.

7. Data Minimisation and Accuracy

- Only data necessary for stated purposes is collected
- Special care is taken for students aged under 16 to obtain parental/carer consent
- All efforts are made to keep data accurate and up to date

8. Retention and Disposal

- The Company maintains a Data Retention Policy (see separate document)
- Personal data is kept only as long as necessary for the purpose
- When no longer needed, data is securely deleted or anonymised

9. Data Security

- Personal data is stored using secure, up-to-date systems
- Access is restricted to authorised personnel
- Regular reviews are conducted of access rights and system integrity
- Backups and disaster recovery procedures are in place
- Data is pseudonymised or encrypted where appropriate

10. Data Sharing and Processors

- Data is only shared externally where lawful and necessary
- All third-party processors are subject to data processing agreements and due diligence
- International data transfers are safeguarded through UK GDPR-compliant mechanisms

11. Data Protection Impact Assessments (DPIAs)

- DPIAs are conducted where high-risk processing is involved (e.g., new technologies, large-scale data use)
- Outcomes are reviewed by the DPO and recorded appropriately

12. Data Breaches

In the event of a breach involving personal data:

- The DPO will assess risk to individuals
- Reportable breaches will be notified to the ICO within 72 hours
- Affected individuals will be informed where there is high risk to their rights and freedoms

13. Training and Awareness

- All staff receive GDPR training at induction and regular refreshers
- Specialist training is provided for high-risk roles (e.g., safeguarding, IT, HR)