

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 when collecting, using, storing, sharing and disposing of personal data.

The Company is committed to protecting the privacy and rights of individuals and ensuring that personal data is processed lawfully, fairly, securely and transparently.

2. Scope

This policy applies to all employees, contractors, consultants and individuals acting on behalf of the Company who process personal data during their work.

It applies to all personal data held or processed by the Company, regardless of format.

3. 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, recording, storage, use, sharing or deletion
- Data Subject: An individual whose data is processed
- **Data Protection Officer (DPO)**
 - Dai Patel
 - Email: dai.patel@nisai.com
 - Tel: 020 8424 8475
- Register of Systems: Internal register of all systems, processes and records where personal data is stored or processed

4. Data Protection Principles

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

1. Processed lawfully, fairly and transparently.
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, including protection against unauthorised access, loss, destruction or damage.

Accountability

The Company is responsible for, and able to demonstrate, compliance with these principles through appropriate policies, procedures, training, records, monitoring and governance arrangements.

5. Responsibilities

Data Protection Officer (DPO)

The DPO is responsible for:

- Overseeing compliance with UK GDPR and data protection legislation.
- Providing advice and guidance on data protection matters.
- Monitoring data protection practices.
- Managing data breach reporting processes.
- Reviewing this policy annually.

Staff Responsibilities

All staff who process personal data must:

- Comply with this policy and related procedures.
- Complete mandatory data protection training.
- Report actual or suspected data breaches immediately.
- Only access personal data required for their role.
- Take reasonable steps to ensure personal data they create, amend or use is accurate and up to date.

Failure to comply with this policy may result in disciplinary action.

6. Lawful Bases for Processing

The Company ensures that all personal data is processed under an appropriate lawful basis, including:

- Consent.
- Contract.
- Legal obligation.
- Vital interests.
- Public task.
- Legitimate interests.

The lawful basis for all processing activities is recorded within the Company's Register of Systems and Records of Processing Activities.

7. Special Category and Criminal Offence Data

The Company processes special category personal data only where a lawful basis under Article 6 UK GDPR and an additional condition under Article 9 UK GDPR applies.

This may include information relating to:

- Health and medical conditions.
- Special Educational Needs and Disabilities (SEND).
- Education, welfare and safeguarding needs.
- Ethnicity and diversity information.
- Other special category data required for lawful educational, employment or welfare purposes.

Criminal offence data will only be processed where authorised by law and where appropriate safeguards are in place.

Personal data relating to safeguarding concerns, child protection, welfare, attendance, health needs and SEND may be processed where necessary to fulfil the Company's legal, safeguarding and educational responsibilities.

8. Rights of the Individual

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

- 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 and profiling

The Company does not routinely undertake solely automated decision-making that produces legal or similarly significant effects on individuals. Where such processing is proposed, appropriate safeguards will be implemented in accordance with UK GDPR requirements.

Subject Access Requests

Requests for access to personal data should be submitted to the DPO.

The Company may request proof of identity before information is disclosed.

Requests will normally be completed within one calendar month unless an exemption applies.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO)

if they are dissatisfied with how their personal data has been handled.

9. Children's Data and Data Minimisation

The Company recognises that children require specific protection regarding their personal data. The Company takes particular care when processing children's personal data and will always consider the best interests, age, understanding and vulnerability of the learner when designing services, communications and data collection processes.

Information provided to learners will be age-appropriate, clear and accessible.

Where consent is relied upon as the lawful basis for processing, appropriate parental or carer consent will be obtained where required by law.

The Company will:

- Collect only personal data necessary for its purposes.
- Ensure personal data remains accurate and up to date.
- Regularly review information held to ensure relevance and accuracy.

10. Records of Processing Activities

The Company maintains Records of Processing Activities (ROPAs) and system registers documenting:

- Purposes of processing.
- Categories of personal data.
- Categories of data subjects.
- Recipients of personal data.
- International data transfers.
- Retention periods.
- Security measures.

These records support compliance with the accountability principle.

11. Retention and Disposal

The Company maintains a separate Data Retention Policy.

Personal data will:

- Be retained only for as long as necessary.
- Be reviewed periodically.
- Be securely deleted, destroyed or anonymised when no longer required.

Disposal methods will be appropriate to the sensitivity of the information.

12. Data Security

The Company implements appropriate technical and organisational measures to protect personal data.

These include:

- Secure systems and devices.
- Role-based access controls.
- Password and authentication controls.
- Encryption and pseudonymisation where appropriate.
- Regular reviews of user access permissions.
- Secure backup arrangements.
- Disaster recovery and business continuity measures.
- Staff awareness and cyber security training.

Detailed security requirements are set out within the Company's Information Security, Acceptable Use, Cyber Security and Business Continuity policies.

13. Data Sharing and Processors

The Company shares personal data only where lawful, necessary and proportionate.

Where third-party processors are used:

- Appropriate due diligence is conducted.
- Written Data Processing Agreements are in place.
- Processors are required to implement suitable security measures.

International Transfers

Where personal data is transferred outside the UK, appropriate safeguards will be implemented in accordance with UK GDPR requirements, including approved transfer mechanisms where necessary.

14. Data Protection Impact Assessments (DPIAs)

The Company conducts Data Protection Impact Assessments where processing is likely to result in a high risk to the rights and freedoms of individuals.

This may include:

- New technologies.
- Large-scale processing.
- Special category data processing.
- System or service changes affecting personal data.

DPIA outcomes will be recorded and reviewed by the DPO.

15. Data Breaches

All actual, suspected or potential personal data breaches must be reported immediately to the DPO.

Upon notification, the Company will:

- Assess the nature and impact of the breach.
- Take action to contain and mitigate risks.
- Record the incident and actions taken.
- Notify the ICO within 72 hours where required.
- Inform affected individuals where there is a high risk to their rights and freedoms.

The Company maintains a separate Data Breach Procedure to support consistent incident management.

16. Training and Awareness

The Company will ensure that:

- All staff receive data protection training during induction.
- Refresher training is provided regularly.
- Specialist training is provided for staff in high-risk roles, including safeguarding, HR and IT.
- Staff remain aware of their responsibilities regarding confidentiality and information security.

17. Monitoring and Compliance

Compliance with this policy will be monitored through:

- Internal audits and reviews.
- Staff training records.
- Data protection impact assessments.
- Breach and incident reporting.
- Management oversight.

Appropriate corrective action will be taken where areas for improvement are identified.

18. Policy Review

This policy will be reviewed annually by the Data Protection Officer, or sooner where there are changes to legislation, regulatory guidance, organisational structure, systems or processing activities.