General Data Protection Regulation (GDPR) Policy

1. Introduction

This GDPR Policy outlines how **Sanako UK Ltd** ("the Company", "we", "us") processes personal data when acting as a software reseller, providing language lab hardware, language-learning software solutions and associated hardware to educational institutions across the United Kingdom and Ireland.

We are committed to ensuring that all personal data is handled in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- EU General Data Protection Regulation (EU GDPR)
- Data Protection Act 2018
- Guidance from the Information Commissioner's Office (ICO) and the Irish Data Protection Commission (DPC)

2. Scope

This policy applies to:

- All personal data processed by the Company
- All staff, contractors, and partners acting on behalf of the Company
- All systems used to store or process personal data
- All customer institutions (schools, colleges, universities)

It covers data processed for:

- Licensing and provisioning of language-learning software
- Customer support and technical assistance
- Account management and billing
- Marketing communications (where consent is obtained)

3. Roles and Responsibilities

Data Controller / Data Processor Status

The Company may act as:

- **Data Processor** when handling personal data on behalf of educational institutions.
- **Data Controller** for internal business operations such as billing, CRM, and marketing.

Data Protection Officer (DPO)

The Company has appointed a DPO.

Contact: Stephen Herndlhofer, stephen.herndlhofer@sanako.com, Sanako UK

4. Types of Personal Data Processed

Educational End Users (Students & Staff)

- Name
- Email address or institutional login ID
- Class or group assignment
- Usage data within the language-learning platform
- Technical logs (IP address, device information)

Institutional Contacts

- Name
- Job title
- Work email address
- Work telephone number
- Contract and billing information

The Company does not intentionally collect special category data unless explicitly authorised by the institution.

5. Legal Basis for Processing

We rely on the following lawful bases:

- **Contractual necessity** – to provide software licences and support
- **Legitimate interests** – service improvement, security, customer relationship management
- **Legal obligation** – compliance with tax, audit, and regulatory requirements
- **Consent** – for optional marketing communications

6. Purpose of Processing

Personal data is processed for:

- Provisioning and managing software licences
- Supporting users and resolving technical issues
- Communicating with institutional contacts
- Monitoring service performance and security
- Managing contracts, invoicing, and renewals
- Providing training and product updates
- Meeting legal and regulatory obligations

7. Data Sharing and Third Parties

We may share personal data with:

- Software vendors and platform providers
- Cloud hosting providers
- Payment processors
- Professional advisors
- Regulatory authorities (where required)

All third parties are bound by GDPR-compliant Data Processing Agreements.

The Company does **not** sell personal data.

8. International Data Transfers

We are not typically required to transfer data outside the UK or EEA.

If we were required by a Client to do so, we will ensure appropriate safeguards such as:

- Adequacy decisions
- Standard Contractual Clauses (SCCs)
- International Data Transfer Agreements (IDTAs)

9. Data Retention

Data Type	Retention Period
Student user accounts	Duration of contract or as instructed by institution
Support tickets	2–3 years
Billing records	6–7 years
CRM/contact data	Until contract ends or consent withdrawn
Technical logs	6–12 months

Data is securely deleted or anonymised after retention periods.

10. Data Security Measures

We implement technical and organisational measures including:

- Encryption of data in transit and at rest
- Role-based access controls
- Multi-factor authentication
- Regular security audits
- Staff GDPR and cybersecurity training

- Secure data-handling procedures
- Incident response and breach reporting processes

11. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Rectify inaccurate data
- Request erasure
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent (where applicable)

Requests should be submitted to: Stephen Herndlhofer, stephen.herndlhofer@sanako.com

Responses are provided within **one month**.

12. Data Breach Procedure

In the event of a personal data breach:

1. The incident is logged and investigated
2. Containment and mitigation actions are taken
3. A risk assessment is completed
4. ICO or DPC notified within **72 hours** (if required)
5. Affected institutions and individuals informed where necessary
6. A post-incident review is conducted

13. Children's Data

As many users are school pupils, we ensure:

- Processing is limited to educational purposes
- No direct marketing to children
- No profiling or automated decision-making affecting children
- Data is processed only under institutional instruction

14. Policy Review

This policy is reviewed **annually** or sooner if:

- Legislation changes
- New systems or vendors are introduced
- Customer requirements change

15. Contact Information

Sanako UK Data Protection Lead:

Stephen Herndlhofer

stephen.herndlhofer@sanako.com