PRIVACY POLICY

Version: 3.0 | Effective Date: 03-11-2026
Stakeholders: Students, Teachers, Administrators, IT Staff, School Leadership, Ministries
Platform: aiSTART – AI Learning Infrastructure

1. INTRODUCTION

Slangit Technologies FZCO ("Slangit", "we", "us" or "our") provides **aiSTART**, an artificial intelligence-enabled education platform designed for schools, educational institutions, teachers, students, parents or guardians, and authorized education stakeholders.
aiSTART may include:

- Artificial intelligence literacy curricula;
- AI-assisted learning and private tutoring tools;
- Educational content and lesson-management features;
- Assignments, projects, assessments and feedback;
- Generative AI tools;
- Gamification and student engagement features;
- School communities and collaboration tools;
- Teacher dashboards and intervention tools;
- Learning analytics and reporting;
- Digital Learning Identity ("DLID") and related educational intelligence features;
- Student safety, safeguarding and risk-detection features; and
- Other educational services introduced from time to time.
-

This Privacy Policy explains how personal information is collected, used, stored, shared and protected when individuals access aiSTART, our websites, including **https://aistart.school**, or related applications and services collectively referred to as the "Services".

This Privacy Policy applies to Slangit and any subsidiary or affiliated entity controlled by Slangit that participates in delivering the Services.

Because aiSTART is primarily provided through schools and educational institutions, the way personal information is managed depends on how a user accesses the platform.

2. OUR ROLE AND THE SCHOOL'S ROLE

2.1. School-managed accounts

Where aiSTART is provided through a school, ministry of education, university, training institution or other educational organization, that organization generally determines:

- Which students, teachers and administrators may use aiSTART;
- What personal information is submitted to the platform;
- Which aiSTART modules and features are activated;
- Who may access student information;
- How long information should be retained;
- Whether parents or guardians receive access, once activated;
- How educational records, analytics and alerts are used; and

- The lawful basis for processing student information.

In these circumstances, the educational institution generally acts as the **data controller**, or equivalent decision-maker under applicable law, and Slangit generally acts as its **data processor or service provider**.

Slangit processes school-managed information only:

- To provide the contracted Services;
- In accordance with the institution's documented instructions;
- As described in this Privacy Policy and the applicable agreement;
- To protect the security and integrity of the Services; or
- Where required or permitted by applicable law.

Requests concerning a school-managed student account should normally be submitted first to the relevant school or educational institution.

2.2. Information controlled directly by Slangit

Slangit may act as the data controller for information relating to:

- Visitors to our public websites;
- Representatives of schools and institutional customers;
- Prospective customers and partners;
- Individuals communicating directly with Slangit;
- Slangit events, demonstrations and marketing activities;
- Customer support and account administration; and
- Accounts offered directly by Slangit, where applicable.

3. USERS OF aiSTART

aiSTART may be used by the following as may be applicable and as the main agreement would be defined:

- Students;
- Teachers;
- School leaders and administrators;
- Counsellors and safeguarding personnel;
- Parents and legal guardians, when access is enabled (currently not activated);
- Ministry or education-authority representatives;
- Trainers and professional-development participants;
- Institutional customer representatives; and
- Authorized Slangit support and operations personnel.

Student accounts are normally created, authorized or managed by the relevant school, or educational institution. Unless otherwise provided, Slangit can provide such accounts if requested by the school or educational institution.

4. PERSONAL INFORMATION WE COLLECT

The information collected depends on the user's role, the features activated by the educational institution and the way aiSTART is configured.

4.1. Student identity and educational information

We may process:

- Student name;
- Email address if available;
- Grade, year group or educational level;
- Class, section or course;
- School or educational institution;
- Country, curriculum and language.

Schools should provide only the information reasonably necessary to operate aiSTART and provide the necessary access.

4.2. Teacher and administrator information

We may collect:

- Name;
- Professional email address;
- School and department;
- Role;
- Classes, courses or students assigned to the user;
- Platform permissions;
- Training participation; and
- Communications with Slangit.

4.3. Learning activity and educational content

aiSTART may process information generated through educational activities, including:

- AI prompts and questions;
- Conversations with AI tutors or assistants;
- Student answers and submissions;
- Assignments, projects and portfolios;
- Assessment responses and results;
- Teacher comments and feedback;
- Generated text, images, presentations, audio, video or code;
- Uploaded documents and files;
- Course participation and completion;
- Accuracy, progress and achievement data;
- Revision and retry patterns;
- Time spent on activities;
- Gamification scores, badges and achievements;
- Community posts and educational discussions; and
- Records of collaboration with teachers or other students.

Users should not submit unnecessary personal, confidential or sensitive information within AI prompts, assignments, community posts or uploaded files.

4.4. Audio, image and multimedia information

Where relevant features are enabled, aiSTART may process subject to compliance with aiSTART policy:

- Images, video, audio or multimedia projects, presentations, websites, uploaded or created by users; and
- Metadata associated with uploaded files.

Camera or microphone access will not be requested through the user's device or browser where required unless it is needed for a specific module that requires such usage.

4.5. Learning analytics and educational insights

aiSTART may generate educational analytics based on a student's interaction with the platform. These may include indicators relating to:

- Course progress;
- Knowledge and skill development;
- Prompt structure and complexity;
- Research and inquiry depth;
- Communication and expression;
- Accuracy and consistency;
- Revision and correction behavior;
- Persistence and completion;
- Engagement patterns;
- Creativity and originality;
- Collaboration;
- Areas of strength;
- Areas in which additional support may be helpful; and
- Changes in learning behavior over time.

These indicators are intended to support education, development and responsible teacher intervention. They are not medical, psychiatric or clinical diagnoses and should not be treated as such.

Teachers, counselors and authorized educational professionals should apply their professional judgment before making decisions based on platform analytics.

4.6. Safety and safeguarding information

Where safeguarding features are enabled, aiSTART may analyze user interactions to identify content that may indicate a potential risk, including references to:

- Self-harm or suicide;
- Violence or threats;
- Abuse, exploitation or grooming;
- Bullying or harassment;
- Sexual exploitation or inappropriate sexual content;
- Hate or discriminatory conduct;
- Dangerous challenges or activities;
- Weapons;
- Illegal conduct;
- Serious threats to a student or another person; or
- Other behavior that may require responsible adult attention.

Where a potential safeguarding concern is detected, aiSTART may:

- Generate a risk indicator;
- Preserve the relevant interaction;
- Notify authorized school safeguarding personnel;
- Present contextual information for human review; or
- Support escalation under the school's safeguarding procedures.

A platform alert is an indicator requiring human review. It is not proof that an incident occurred, a disciplinary finding or a medical diagnosis.
aiSTART is not an emergency service and should not be relied upon as the only mechanism for protecting a student. Schools remain responsible for maintaining appropriate safeguarding policies, trained personnel and emergency procedures.
Where permitted or required by law, information may be disclosed to appropriate authorities where Slangit reasonably believes that disclosure is necessary to protect a person from an imminent and serious risk of harm.

4.7. Device, technical and usage information

We may automatically collect:

- IP address;
- Device type;
- Operating system;
- Browser type and version;
- Language and time-zone settings;
- Device identifiers;
- Login date and time;
- Session duration;
- Pages and platform features accessed;
- Error and diagnostic information;
- Network and performance data;
- Security events;
- General location derived from an IP address, such as country, city or region; and
- Interactions with platform notifications.

We do not require precise geolocation for the ordinary delivery of aiSTART unless a specific feature clearly requires it and appropriate authorization has been obtained.

4.8. Support and communication information

We may retain:

- Support requests;
- Emails and messages;
- Feedback and survey responses;
- Complaints;
- Training requests;
- Technical troubleshooting information; and
- Records of communications with schools, parents, teachers or other users.

4.9. Institutional and payment information

For institutional customers, we may collect:

- Organization name and address;

- Authorized representative information;
- Contract and subscription information;
- Billing contacts;
- Purchase orders relevant to us;
- Invoices relevant to us;
- Payment status relevant to us; and
- Transaction references.

Students are not asked to provide payment information.

5. HOW WE COLLECT INFORMATION

We may collect information:

- Directly from the user;
- From the school or educational institution;
- From teachers and school administrators;
- Automatically through use of the Services;
- Through authorized integrations with school systems;
- From identity or single-sign-on providers;
- From learning-management or student-information systems;
- Through customer support and training activities; or
- From authorized business partners and resellers.

Where information is provided through an integration, the institution is responsible for ensuring that it has authority to connect the system and transfer the relevant information.

6. HOW WE USE PERSONAL INFORMATION

6.1. Delivering aiSTART

We use personal information to:

- Create and manage accounts;
- Authenticate users;
- Assign roles and permissions;
- Provide courses, lessons and educational tools;
- Deliver AI-generated responses;
- Process assignments and assessments;
- Provide feedback and learning support;
- Track course and curriculum progress;
- Enable administrators, teachers, students and parent dashboards, as may be applicable;
- Support student projects and collaboration;
- Operate assessments, gamification and other features; and
- Provide technical and customer support.

6.2. Personalizing learning

We may use learning activity to:

- Adapt explanations to a student's educational level;
- Recommend relevant learning activities;
- Identify areas in which further practice may be useful;
- Provide progress information;

- Help teachers understand student engagement;
- Support responsible teacher intervention; and
- Improve the accessibility and relevance of educational content.

Personalization is intended to assist educators and students, not replace teachers or professional educational judgment.

6.3. Assessments and educational reporting

We may process information to:

- Administer assessments;
- Calculate results;
- Generate progress reports, if applicable;
- Provide teacher dashboards;
- Compare performance against assigned learning outcomes;
- Support curriculum evaluation;
- Generate school-level or class-level analytics; and
- Assist institutions in evaluating program effectiveness.

Where possible, institutional reports are aggregated or de-identified.

6.4. Student safety

We may use information to:

- Detect potential safeguarding concerns;
- Reduce harmful or inappropriate use of AI;
- Apply content guardrails;
- Prevent misuse of the platform;
- Notify authorized safeguarding personnel;
- Investigate security or safety incidents.

6.5. Platform security and administration

We may process information to:

- Prevent unauthorized access;
- Detect fraud, abuse and cyberattacks;
- Maintain audit and security logs;
- Diagnose technical issues;
- Develop back-up and restore the Services;
- Enforce platform terms and institutional agreements; and
- Maintain service reliability.

6.6. Research and service improvement

We may use aggregated, statistical or appropriately de-identified information to:

- Evaluate platform performance;
- Improve educational content;
- Improve accessibility;
- Measure system reliability and response quality;
- Identify general educational trends;
- Develop new educational features; and
- Conduct internal research.

We do not attempt to re-identify information that has been properly de-identified.

6.7. Legal and regulatory purposes

We may process information to:

- Comply with applicable laws;
- Respond to lawful requests;
- Establish, exercise or defend legal claims;
- Conduct compliance reviews;
- Protect legal rights;
- Investigate unlawful conduct; and
- Meet contractual and regulatory obligations.

7. LAWFUL BASIS FOR PROCESSING

Depending on the jurisdiction and circumstances, personal information may be processed on the basis of:

- Performance of a contract;
- The institution's educational function or public task;
- Compliance with a legal obligation;
- Legitimate interests that do not override the individual's rights;
- Consent from the user, parent or guardian;
- Authorization provided by a school where legally permitted;
- Protection of vital interests; or
- Another lawful basis recognized under applicable law.

The relevant school or educational institution is responsible for identifying and documenting the appropriate lawful basis for school-controlled processing. Where consent is required, consent must be informed, freely given and capable of being withdrawn.

8. USE OF ARTIFICIAL INTELLIGENCE

aiSTART uses artificial intelligence to provide educational functions such as:

- Answering student questions;
- Explaining concepts;
- Supporting research;
- Generating learning content;
- Assisting with projects;
- Providing formative feedback;
- Analysing learning interactions;
- Applying safety guardrails; and
- Helping teachers understand student progress.

AI-generated content may occasionally be incomplete, inaccurate, inappropriate or misleading. Users should verify important information, and teachers should supervise the educational use of AI.

Slangit does not represent AI-generated outputs as a substitute for:

- A teacher;
- A school counsellor;
- A psychologist or medical professional;
- A safeguarding professional;

- Legal advice;
- Emergency services; or
- Human decision-making.

8.1. No training on identifiable customer content

Slangit does not use identifiable student, teacher or institutional content to train general-purpose artificial intelligence models.
We do not authorize contracted third-party AI providers to use aiSTART customer prompts, responses or uploaded content to train their general-purpose models.
Depending on the aiSTART configuration, prompts or content may be securely transmitted to contracted technology or AI providers solely to generate the requested response or deliver the relevant platform feature.
Aggregated or properly de-identified technical and usage information may be used to improve security, reliability, educational quality and platform performance.

8.2. Automated analysis

aiSTART may automatically analyze learning activity and generate recommendations, indicators or risk alerts.
Slangit does not intend for aiSTART to make decisions producing legal or similarly significant effects on a student without meaningful human involvement.
Schools must ensure that teachers, counselors or authorized personnel review relevant information before it is used for:

- Disciplinary action;
- Academic placement;
- Admission or exclusion;
- Special educational designation;
- Psychological or medical conclusions; or
- Other significant decisions affecting a student.

9. CHILDREN'S PRIVACY AND PARENTAL AUTHORIZATION

aiSTART is designed for educational use and may be used by children and teenagers.
Student accounts must be established through:

- A participating school or educational institution;
- An authorized education authority; or
- Another process permitted by applicable law.

Where parental or guardian consent is legally required, the school and Slangit will allocate responsibility for obtaining and documenting that consent under the applicable agreement and law.
Where a school is legally permitted to authorize educational technology on behalf of parents, the information may only be used for the authorized educational purpose and not for unrelated commercial purposes.
Slangit will not knowingly permit a child below the applicable minimum age to create an independent account without required school or parental authorization.
Where we learn that a child's information has been collected without the required authorization, we may suspend the account and delete or return the information as appropriate.

Parents and guardians should contact the student's school regarding:

- Access to student information;
- Correction of school records;
- Account deletion;
- Withdrawal of consent;
- Questions about classroom use; or
- Concerns about educational analytics.

Slangit may refer such requests to the institution where the institution controls the relevant information.

10. HOW WE SHARE PERSONAL INFORMATION

We do not sell student personal information.
We do not use student information for targeted advertising.
We do not disclose student information to advertisers or data brokers.
We may share personal information with the following parties where necessary.

10.1. Schools and authorized educational personnel

Student information may be available to authorized:

- Teachers;
- School administrators;
- Counsellors;
- Safeguarding personnel;
- Education-authority representatives; and
- Other persons authorized by the institution.

Access is determined by user roles, permissions, contractual requirements and institutional instructions.

10.2. Service providers and subprocessors

We may use service providers for:

- Cloud hosting;
- Data storage;
- Cybersecurity;
- Authentication;
- Email and communications;
- Technical support;
- Artificial intelligence processing;
- Speech, audio or image processing;
- Performance monitoring;
- Backup and disaster recovery; and
- Payment processing for institutional customers.

These providers are permitted to process information only for the contracted service and are subject to appropriate confidentiality, data-protection and security obligations.
A list of material subprocessors may be made available to institutional customers upon request or through Slangit's published subprocessor documentation.

10.3. Affiliates

Information may be shared with Slangit affiliates where necessary to operate, support or secure aiSTART, subject to equivalent privacy and confidentiality obligations.

10.4. Professional advisors

We may share information with legal, accounting, insurance, audit, cybersecurity or compliance advisors where reasonably necessary.

10.5. Legal and safety disclosures

We may disclose information where we reasonably believe disclosure is necessary to:

- Comply with a legal obligation;
- Respond to a lawful government or court request;
- Protect a child or another person from serious harm;
- Investigate abuse, fraud or a security incident;
- Protect the rights and property of Slangit, its customers or users; or
- Enforce applicable agreements.

10.6. Business transfers

Information may be transferred as part of a merger, financing, restructuring, acquisition or sale of all or part of Slangit's business.
Any successor will remain subject to applicable data-protection requirements and contractual restrictions relating to student information.

11. INTERNATIONAL DATA TRANSFERS AND HOSTING

Slangit provides its Services in multiple countries. Personal information may be hosted or processed in countries other than the user's country of residence, depending on:

- The customer's deployment configuration;
- The selected cloud or hosting environment;
- Contractual requirements;
- Data-residency requirements; and
- The locations of authorized service providers.

Where required, we use appropriate contractual, organizational and technical safeguards for international data transfers.
Institutional customers may request information about:

- Available hosting regions;
- Data residency;
- Sub-processors;
- International transfer mechanisms; and
- On-premises or dedicated deployment options.

12. DATA RETENTION

We retain personal information only for as long as reasonably necessary to:

- Provide the Services;
- Fulfil the educational purpose;
- Follow the institution's instructions;
- Maintain security and audit records;
- Resolve disputes;

- Meet contractual requirements; and
- Comply with applicable law.

For school-managed accounts, retention periods may be established in the customer agreement, data-processing agreement or documented institutional instructions.
Following the termination of an institutional agreement, Slangit may:

- Return or export customer information;
- Delete active customer information;
- Retain information temporarily within protected backups;
- Retain legally required records; or
- Retain properly aggregated or de-identified information.

Backup information is deleted or overwritten in accordance with Slangit's backup cycle, unless longer retention is required by law or necessary to investigate a security or safeguarding incident.
Safeguarding records may be subject to different retention requirements due to the nature of the information and the school's legal responsibilities.

13. DATA SECURITY

We use organizational, technical and physical safeguards designed to protect personal information against:

- Unauthorized access;
- Accidental loss;
- Misuse;
- Alteration;
- Improper disclosure; and
- Destruction.

Measures may include:

- Role-based access controls;
- Authentication and password controls;
- Encryption in transit and, where appropriate, at rest;
- Security logging and monitoring;
- Network and infrastructure protections;
- Secure software-development practices;
- Backup and disaster-recovery procedures;
- Staff confidentiality requirements;
- Supplier-security assessments; and
- Incident-response procedures.

Access to student information is limited to personnel and service providers who require access for an authorized purpose.
No online service can guarantee absolute security. Schools and users must protect passwords, devices and account credentials and promptly report suspected unauthorized access.

14. PERSONAL DATA INCIDENTS

Where Slangit becomes aware of a personal data breach, we will:

- Investigate the incident;
- Take reasonable containment and remediation measures;

- Preserve relevant evidence;
- Notify the institution without undue delay, and within 72 hours where the law requires;
- Support the institution in meeting its legal obligations; and
- Notify regulators or affected individuals where Slangit is legally responsible for doing so.

Schools should immediately report suspected security or privacy incidents to Slangit using the contact provided herein.

15. COOKIES AND SIMILAR TECHNOLOGIES

We may use cookies, local storage and similar technologies to:

- Maintain user sessions;
- Authenticate users;
- Remember preferences;
- Protect accounts;
- Measure platform performance;
- Diagnose errors;
- Understand general website usage; and
- Improve the Services.

Student-facing areas do not use cookies for targeted advertising.

Our public website may use limited analytics or marketing technologies directed toward adult institutional visitors, subject to applicable consent requirements.

Users may adjust browser settings to block or delete cookies. Blocking essential cookies may prevent certain aiSTART functions from operating correctly.

16. MARKETING COMMUNICATIONS

We may send service information and relevant communications to adult representatives of schools, prospective institutional customers, partners and professional users.

Recipients may unsubscribe from non-essential marketing communications by:

- Using the unsubscribe link in the message; or
- Contacting Slangit at aistart@slangit.ai.

Service, security, account and contractual notices cannot always be disabled while an account or institutional relationship remains active.

We do not use school-managed student contact information for direct commercial marketing.

17. YOUR PRIVACY RIGHTS

Depending on applicable law, individuals may have the right to:

- Request access to personal information;
- Request correction of inaccurate or incomplete information;
- Request deletion;
- Request restriction of processing;
- Object to certain processing;
- Withdraw consent;
- Request transfer or portability of information;
- Request information about automated processing;
- Challenge a decision based solely on automated processing;
- Submit a complaint to a data-protection authority; and
- Request information about international transfers.

These rights may be limited where information must be retained for:

- Legal compliance;
- School-record obligations;
- Safeguarding;
- Security;
- Fraud prevention;
- Establishment or defense of legal claims; or
- Protection of another person.

17.1. School-managed accounts

Where information is controlled by a school or educational institution, the request should be submitted to that institution. Slangit will reasonably assist the institution in responding to valid requests in accordance with the applicable agreement and law.

17.2. Identity verification

Before completing a privacy request, Slangit or the institution may request information necessary to confirm:

- The requester's identity;
- Authority over the relevant account; and
- A parent or guardian's relationship to the student.

No fee is normally charged for exercising privacy rights. A reasonable fee may be charged, or a request may be refused, where permitted by law and where the request is manifestly unfounded, excessive or repetitive.

18. THIRD-PARTY SERVICES AND LINKS

aiSTART may integrate with or contain links to third-party services, including:

- School information systems;
- Single-sign-on providers;
- Learning-management systems;
- External educational resources;
- Video or communication platforms; and
- Content or productivity tools selected by the institution, if applicable.

Where a third-party service is independently selected or controlled by the institution or user, that third party's privacy policy will apply.

Slangit is not responsible for the independent privacy practices of third parties that are not acting as Slangit service providers.

19. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy to reflect:

- Changes to aiSTART;
- New educational or safety features;
- Changes in our processing practices;
- Changes in applicable law; or
- Improvements to privacy and security protections.

The updated version will show a revised effective date.

Where changes materially affect student information or institutional responsibilities, we may also notify the relevant institutional customer and request updated authorization where required.

20. APPLICABLE LAWS

Slangit complies with the UAE Personal Data Protection Law, Federal Decree-Law No. 45 of 2021 (PDPL), and is designed around the principles of the EU General Data Protection Regulation (GDPR).

Where a deployment is within the Dubai International Financial Centre (DIFC) or the Abu Dhabi Global Market (ADGM), the data protection rules of those jurisdictions also apply: DIFC Law No. 5 of 2020 (Data Protection Law) and the ADGM Data Protection Regulations 2021.

Slangit is also designed to comply with the local data protection laws and regulations of each country where aiSTART is deployed.

21. CONTACT US

Questions, concerns or requests relating to this Privacy Policy may be submitted to:
Slangit Technologies FZCO
Email: aistart@slangit.ai

For school-managed accounts, students and parents should normally contact the school before contacting Slangit. When contacting us, please do not include unnecessary student information or sensitive safeguarding details in an unsecured email.

****