



POLICY

ARTIFICIAL INTELLIGENCE USE POLICY

Change begins with Education

TABLE OF CONTENTS

1 STUDYBEYONDBORDERS IN CAMBODIA OVERVIEW	1
2 PURPOSE	1
3 SCOPE	2
4 GUIDING PRINCIPLES	2
4.1. Integrity and truthfulness	2
4.2. Human accountability	2
4.3. Transparency	2
4.4. Do no harm	2
4.5. Legal compliance	2
4.6. Continuous improvement	3
4.7. Risk-based approach	3
5 ACCEPTABLE AND PROHIBITED USES	3
5A. Prohibited AI practices (EU AI Act, Article 5)	4
6 ETHICAL COMMUNICATION — MANDATORY RULES	4
6A. Transparency and disclosure (EU AI Act, Article 50)	5
7 DATA PROTECTION AND PRIVACY	5
8 ROLES AND RESPONSIBILITIES	6
9 AI USAGE REGISTER	7
10 TRAINING AND AWARENESS	7
11 MONITORING, INCIDENTS, AND REVIEW	8
12 NON-COMPLIANCE	8
13 STATEMENT OF COMMITMENT	8
14 JURISDICTIONAL APPLICATION OF THIS POLICY	9
15 POLICY MANAGEMENT	11
ANNEX A. AI RISK ASSESSMENT FRAMEWORK	12
A.1 Risk tiers and controls	12
A.2 Assessment workflow	12

ARTIFICIAL INTELLIGENCE USE POLICY

Aligned with ISO/IEC 42001:2023 — Artificial Intelligence Management Systems (AIMS), and Regulation (EU) 2024/1689 (the EU AI Act), with proportionate application across all operating jurisdictions

1 STUDYBEYONDBORDERS IN CAMBODIA OVERVIEW

StudyBeyondBorders in Cambodia (**SBBC**) is a local Cambodian non-government organisation operating in rural areas of Battambang, Oddar Meanchey, and Siem Reap Provinces. The organisation is supported by an alliance of registered development organisations in Australia (**SBBA**), the UK (**SBBUK**), and Ireland (**SBBI**).

SBBC aims to build capability within Cambodian education policy-making, leadership, mentoring, and training to equip and motivate teachers to provide quality education to children. The organisation is committed to supporting systemic change so that educators are proud to work in the teaching profession and are highly respected by parents, communities, and peers. To this end, **SBBC** conducts programs to mentor education leaders, upskill teachers, engage parents and communities, and develop resources that together enable the delivery of quality education to schoolchildren. The organisation seeks to embed all its work at the school, district, provincial, and national levels.

2 PURPOSE

This policy sets out how **SBBC** uses artificial intelligence (AI) responsibly, ethically, and transparently in support of our mission to deliver educational projects and research in Cambodia and to raise funds internationally.

SBBC may use AI to assist or produce documentation outputs, program updates and financial data that is used in Cambodia, Ireland (EU), UK, and Australia. As such there is an obligation for AI and privacy compliance across multiple justifications. This policy sets out how **SBBC** meets those compliance obligations.

The policy is aligned with ISO/IEC 42001:2023, the international standard for AI Management Systems (AIMS), and reflects our commitment to donor trust, beneficiary protection, and the highest standards of ethical communication.

It is also aligned with Regulation (EU) 2024/1689 (the “EU AI Act”), the principal obligations of which apply from 2 August 2026. The Organisation operates as a “deployer” (not a “provider”) of AI systems within the meaning of the EU AI Act, and the framework set out in this policy is applied proportionately for each operating jurisdiction (Ireland and the wider EU, the United Kingdom, Australia and Cambodia) on the basis of a single common control set with jurisdiction-specific overlays, see Section 14 (Jurisdictional Application) and Annex A (AI Risk Assessment Framework).

3 SCOPE

This policy applies to all staff, trustees, volunteers, and contractors of the Organisation. It covers all uses of AI tools in:

- Internal operations, including drafting, research, translation, and administration
- Fundraising and donor communications across all jurisdictions
- Educational and research programme content developed in, for or about Cambodia
- Grant applications, impact reporting, and regulatory submissions

4 GUIDING PRINCIPLES

4.1. **Integrity and truthfulness**

AI must never be used to create misleading, exaggerated, or false information about beneficiaries, projects, outcomes, or impact. All factual claims in AI-assisted content must be independently verifiable before use.

4.2. **Human accountability**

All AI-generated content must be reviewed and approved by a named staff member before use. Final responsibility for any output rests with the staff member, not the AI tool. AI systems do not hold accountability — people do.

4.3. **Transparency**

The Organisation will be open about its use of AI where this is material to its communications and programmes. Where AI has made a material contribution to donor-facing content, this must be acknowledged in internal records and, where appropriate, disclosed externally.

4.4. **Do no harm**

AI must not be used in ways that exploit vulnerable individuals or communities, reinforce bias or discrimination, misrepresent cultural or social contexts, or cause reputational, financial, or personal harm to any person connected with the Organisation's work.

4.5. **Legal compliance**

AI use must comply with applicable data protection and AI-related law in all operating jurisdictions, including GDPR (Ireland and EU), the UK Data Protection Act 2018, the Australian Privacy Act 1988, and Cambodian data protection requirements (Personal Data Protection Law 2024).

In the EU, AI use must additionally comply with Regulation (EU) 2024/1689 (the EU AI Act). The Organisation acknowledges that the prohibitions in Article 5 and the AI literacy obligation in Article 4 have applied since 2 February 2025, that obligations on general-purpose AI (GPAI) models have applied since 2 August 2025, and that the principal obligations on deployers, the transparency rules in Article 50 and the governance, market-surveillance and penalty provisions become enforceable from 2 August 2026.

In the United Kingdom, AI use must follow the principles-based, regulator-led approach of the UK government's AI Regulation White Paper and the guidance of the Information Commissioner's Office, the Equality and Human Rights Commission, and other competent UK regulators.

In Australia, AI use must follow the Australian Government's Voluntary AI Safety Standard (2024), the AI Ethics Principles, and any mandatory guardrails for high-risk AI as they enter into force, in addition to obligations under the Privacy Act and the Online Safety Act.

In Cambodia, AI use must comply with the Personal Data Protection Law 2024 and any further AI-specific guidance issued by the Royal Government of Cambodia.

4.6. Continuous improvement

The Organisation will review and update its AI governance practices as AI use develops, as regulations evolve, and as lessons are learned from operational experience.

4.7. Risk-based approach

The Organisation adopts the risk-tiered approach of the EU AI Act as the common framework for governing AI use across all jurisdictions. Each AI use case is classified into one of four tiers: unacceptable, high, limited, or minimal risk, using the AI Risk Assessment Framework at Annex A. Controls scale with the assessed tier: unacceptable-risk practices are prohibited outright (Section 5A); high-risk uses require explicit **AIMS Owner** sign-off, a documented Fundamental Rights and Data Protection Impact Assessment (FRIA / DPIA), human oversight under Article 14 / Article 26 of the EU AI Act, and registration in the AI Usage Register; limited-risk uses must comply with the transparency obligations in Section 6A; and minimal-risk uses follow the standard human-review, accuracy and data-protection rules in this policy.

5 ACCEPTABLE AND PROHIBITED USES

AI may be used to support	AI must not be used to
Drafting emails, reports, funding applications, and programme materials	Invent or fabricate stories, quotes, statistics, or beneficiaries
Summarising research and literature	Make decisions affecting individuals without human oversight
Administrative and operational efficiency tasks	Process sensitive personal data without explicit authorisation
Translation of documents (with cultural review)	Generate synthetic representations of beneficiaries without consent

Initial drafts of donor or stakeholder communications	Circumvent human decision-making in safeguarding processes
Internal data analysis (anonymised data only)	Present AI-generated content as sole original human work in formal contexts

5A. Prohibited AI practices (EU AI Act, Article 5)

In addition to the prohibitions in Section 5, the following AI practices are prohibited under Article 5 of the EU AI Act and are prohibited Organisation-wide regardless of the jurisdiction in which the activity takes place. Although Article 5 is binding only within the EU, the Organisation applies these prohibitions globally as a matter of policy because they reflect the Organisation's ethical standards and reduce the risk of cross-border non-compliance:

- Subliminal, manipulative or deceptive AI techniques that materially distort the behaviour of donors, beneficiaries, students or staff in a way likely to cause harm.
- Exploitation of vulnerabilities arising from age, disability, or social or economic situation. This is particularly relevant given the Organisation's work with children, families and rural communities in Cambodia, and any AI use case that targets such groups must be escalated to **the AIMS Owner**.
- Social scoring of individuals or groups based on social behaviour or personal characteristics that leads to detrimental treatment.
- Untargeted scraping of facial images from the internet or CCTV to build or expand facial recognition databases.
- Emotion-recognition AI in the workplace or educational settings, except where strictly necessary for medical or safety reasons. This restriction applies to volunteers and Cambodian school programmes as well as to staff.
- Biometric categorisation that infers or assigns sensitive attributes such as race, political opinions, trade-union membership, religious or philosophical beliefs, sex life or sexual orientation.
- Predictive risk scoring of individuals to forecast criminal behaviour based solely on profiling or personality traits.
- Real-time remote biometric identification of individuals in publicly accessible spaces.

Any proposal to use, procure, fund or pilot an AI system that may fall within the categories above must be referred to **the AIMS Owner** before any commitment is made. Penalties under the EU AI Act for breach of Article 5 can reach €35 million or 7% of worldwide annual turnover, whichever is higher.

6 ETHICAL COMMUNICATION — MANDATORY RULES

Given the Organisation's ethical communication mandate and its fundraising activities across multiple jurisdictions, the following rules are mandatory for all external communications:

- No fictional or composite beneficiaries may be portrayed unless explicitly and prominently disclosed as such.
- No unverifiable claims, statistics, or impact assertions may be published or distributed.
- All impact statements must be fact-checked against source data before publication.
- Language must respect the dignity, agency, and cultural context of the communities the Organisation serves.
- AI-drafted fundraising content must pass human editorial review before distribution to donors or funders;
- Staff must not use AI to generate content that implies endorsements, quotes, or permissions not actually given.

6A. Transparency and disclosure (EU AI Act, Article 50)

From 2 August 2026, Article 50 of the EU AI Act imposes specific transparency obligations on deployers of certain AI systems. The Organisation applies the following rules globally for consistency:

- **Chatbots and conversational interfaces:** where the Organisation deploys an AI system that interacts directly with donors, supporters, beneficiaries or members of the public, users must be clearly informed at the start of the interaction that they are dealing with an AI system, unless this is obvious from the context.
- **Synthetic or AI-manipulated images, audio and video (“deepfakes”):** any AI-generated or AI-manipulated image, audio or video used in fundraising, advocacy, campaigns or programme reporting that depicts real persons, places or events, or that could plausibly be mistaken for an authentic recording, must be clearly and visibly labelled as AI-generated or AI-manipulated. Synthetic representations of beneficiaries are prohibited under Section 5 except where editorially justified, explicitly labelled, and approved in writing by **the AIMS Owner**.
- **AI-generated text published to inform the public on matters of public interest** (e.g. published articles, position papers, public-facing impact statements) must disclose that the text was generated or substantially generated by AI, unless the content has undergone meaningful human review and editorial responsibility has been formally taken by a named staff member, in which case the human-review record stands as the basis for accountability.
- **Emotion-recognition and biometric-categorisation systems** (where lawfully used): individuals exposed to such systems must be informed of their operation. The Organisation does not currently deploy such systems and any proposed deployment is subject to **the AIMS Owner** approval and Section 5A.
- **Disclosure must be in plain language, in the language of the audience** (English, and Khmer where the audience is in Cambodia), and must be accessible to persons with disabilities so far as reasonably practicable.

7 DATA PROTECTION AND PRIVACY

AI tools process data in ways that may create legal obligations. The following requirements apply without exception:

- **Personal data restriction:** Personal data: including donor, beneficiary, student, staff, or partner data, must not be entered into any AI tool unless **the General Manager-Shared Services (AIMS Owner)** has authorised this and confirmed that an adequate Data Processing Agreement is in place with the tool's provider.
- **Anonymisation requirement:** Where AI tools are used to analyse or process data, all identifiable information must be anonymised or pseudonymised before input unless otherwise explicitly authorised.
- **Jurisdiction awareness:** Staff using AI tools in connection with data relating to persons in Ireland, the UK, or Australia must be aware of the applicable data protection regime and seek guidance where uncertain.
- **Cambodia programme data:** Data relating to beneficiaries in Cambodia is subject to enhanced protection given the potentially vulnerable context. Such data requires explicit **AIMS Owner** sign-off before any AI assisted processing.
- **Cloud tool risk:** Commercial AI tools (including generative AI services) hosted outside the European Economic Area (EEA) may not provide adequate data protection guarantees without appropriate contractual safeguards. Staff must seek guidance before using such tools with any personal information.
- **Software usage:** Where **SBBC** is providing an employee with an AI tool (or funding access) then the user account must be linked to a SeeBeyondBorders email address, not a personal use email. This ensures that any content shared with an AI software is governed by this **AI Policy** and associated Data Protection and Privacy.

8 ROLES AND RESPONSIBILITIES

Role	Responsibilities
Board of Trustees	Ultimate accountability for ethical AI governance; formal policy approval; annual oversight review.
General Manager-Shared Services (AIMS Owner)	Day-to-day AIMS ownership; policy enforcement; escalation point; annual report to Board.
IT and Facilities Manager (AI Responsible Person)	Maintain AI tool register and risk register; monitor compliance; coordinate training; report incidents. Confirm the Organisation's role under EU AI Act Article 3 (deployer / provider / distributor / importer) for each tool, run the



	Annex A risk assessment, escalate prohibited or high-risk proposals to the AIMS Owner , and maintain Article 50 disclosures and Article 4 AI literacy records.
All Staff, Volunteers & Contractors	Follow this policy; apply human review gates; exercise judgement; escalate concerns promptly.

9 AI USAGE REGISTER

The AI Responsible Person shall maintain a central AI Usage Register recording all AI tools approved for use by the Organisation. The register must capture, at minimum:

- Tool name and provider
- Purpose and function
- Assessed risk level (low / medium / high)
- Personal data processing: yes / no
- Data Processing Agreement in place: yes / no / not required
- Named responsible person for each tool
- Date of last review
- EU AI Act risk classification (unacceptable / high / limited / minimal) — see Annex A
- Role of the Organisation in respect of the tool: deployer / provider / distributor / importer (under EU AI Act, Article 3)
- Whether the underlying model is a general-purpose AI (GPAI) model and, if so, whether it is identified as a GPAI model with systemic risk
- Operating jurisdiction(s) where the tool is used (EU / UK / Australia / Cambodia / global) and whether outputs are intended to be used in the EU
- Article 50 transparency obligation triggered (yes / no), and how the disclosure is made
- For high-risk uses: link to the Fundamental Rights and Data Protection Impact Assessment (FRIA / DPIA) and the human-oversight arrangements

No new AI tool may be used by staff until it has been added to the register and reviewed by the AI Responsible Person. The register must be reviewed at least quarterly and maintained as a live document.

10 TRAINING AND AWARENESS

All personnel — including trustees — **must**:

- Complete basic AI literacy and awareness training within 60 days of this policy taking effect (or within 30 days of joining the Organisation). This satisfies the Organisation's obligation under Article 4 of the EU AI Act, which has applied since 2 February 2025 and requires deployers to ensure a sufficient level of AI literacy among staff and other persons operating AI systems on their behalf, taking into account their technical knowledge, experience, education and the context in which the AI

systems are used. Training content and frequency must be proportionate to role and risk exposure, and training is mandatory (not optional) for all staff with access to AI tools, including volunteers and contractors.

- Understand the risk of inaccurate or fabricated AI outputs (commonly referred to as hallucinations) and apply appropriate critical scrutiny.
- Know when AI tools are and are not appropriate for a given task.
- Understand when usage of AI tools can contribute meaningfully to the organization's mission, while considering its potential environmental impact and whether a particular task is better suited to the use of simpler methods that can achieve the same results.
- Know how and to whom to escalate concerns about AI use.

Training records must be maintained by the AI Responsible Person and reviewed annually.

11 MONITORING, INCIDENTS, AND REVIEW

- **Quarterly monitoring:** The **AI Responsible Person** will review AI tool usage against the register and report any anomalies or emerging risks to the GM Shared Services each quarter.
- **Incident reporting:** Any incident arising from AI use — including data breaches, publication of inaccurate content, or reputational concerns — must be reported immediately to **the General Manager-Shared Services**, who will assess whether regulatory notification is required under applicable law.
- **Annual policy review:** This policy will be reviewed annually, timed to coincide with the Board's annual governance review cycle. **The General Manager-Shared Services** will present an AI governance summary to the Board at this review.
- **Ad hoc review:** This policy may be reviewed earlier in response to material changes in the Organisation's AI use, a significant incident, or substantive changes in applicable law or regulation.

12 NON-COMPLIANCE

Failure to comply with this policy may result in:

- Withdrawal of access to AI tools.
- Mandatory retraining.
- Disciplinary action in accordance with the Organisation's HR policies.
- Escalation to trustees where the breach involves a significant ethical, legal, or reputational risk.

13 STATEMENT OF COMMITMENT

SBBC is committed to using AI responsibly to enhance its mission while maintaining the highest standards of integrity, accountability, and respect for the communities it serves in Cambodia and across all jurisdictions where it operates. This policy reflects both our legal obligations and our organisational values.

14 JURISDICTIONAL APPLICATION OF THIS POLICY

The Organisation operates a single AI governance framework, anchored on ISO/IEC 42001:2023 and the EU AI Act, and applies it proportionately in each jurisdiction. The same Risk Assessment (Annex A), AI Usage Register (Section 9), AI literacy training (Section 10), and incident reporting workflow (Section 11) are used everywhere. The table below sets out the additional, jurisdiction-specific obligations that apply on top of the common framework. Where jurisdictions diverge, the strictest applicable standard is followed for any cross-border activity.

Jurisdiction	Primary applicable AI / data law	Local overlay on this policy
Ireland / EU	EU AI Act (Reg. (EU) 2024/1689); GDPR (Reg. (EU) 2016/679); Irish Data Protection Act 2018; ePrivacy Regulations.	Full application of Sections 4A (Article 5 prohibitions), 5A (Article 50 transparency) and 9 (Article 4 AI literacy). Any high-risk use under Annex III triggers deployer obligations under Article 26: human oversight, input-data quality checks, monitoring, logging, FRIA where required, and notification of serious incidents to the national competent authority within 15 days. Personal data is processed under GDPR; DPIA required for high-risk processing.
United Kingdom	UK GDPR; Data Protection Act 2018; Equality Act 2010; Online Safety Act 2023; ICO AI guidance and the cross-regulator principles in the UK Government's AI Regulation White Paper.	The UK has no equivalent to the EU AI Act. The Organisation voluntarily applies the EU AI Act framework as best practice. The five UK cross-sector principles (safety/security/robustness; appropriate transparency and explainability; fairness; accountability and governance; contestability and redress) are treated as satisfied by adherence to this policy. The EU AI Act may still apply extra-territorially where outputs are used in the EU (Article 2(1)(c)).
Australia	Privacy Act 1988 (as amended); Online Safety Act 2021; Australian AI Ethics Principles; Voluntary AI Safety Standard 2024; ACNC governance standards;	SeeBeyondBorders Australia is a small charity (less than 50 staff worldwide) and is currently below most thresholds for mandatory AI-specific obligations, but adopts the Voluntary AI Safety Standard's 10 guardrails through this policy. ACNC governance standards on accountability and risk management

	emerging mandatory guardrails for high-risk AI.	apply. Privacy Act notifiable data breaches involving AI must be reported to the OAIC within 30 days.
Cambodia	Personal Data Protection Law 2024; Law on E-Commerce 2019; Cybercrime Law (draft); MoU obligations with the Ministry of Education, Youth and Sport (MoEYS) and the Council for the Development of Cambodia (CDC).	No AI-specific statute is in force. The Organisation applies the Section 5A prohibitions and the EU/AU framework as the higher standard. Beneficiary data, particularly children's data, is treated as enhanced risk and may not be processed by AI tools without written AIMS Owner approval (Section 7). Disclosures under Section 6A are translated into Khmer.

Cross-border note: when the Organisation acts in one jurisdiction but its AI use produces outputs (text, images, decisions) intended for use in another, the AI Responsible Person determines the applicable regime by reference to where the output is used and who is affected. Where any output is used or any individual affected is in the EU, the EU AI Act applies in addition to local law (extra-territorial effect, EU AI Act Article 2(1)(c)).

15 POLICY MANAGEMENT

This policy has been approved by **the Board of Trustees of SBBC** as noted below.

Amendments will be recommended to **the Managing Director** from time to time as deemed appropriate by **the General Manager-Shared Services**, usually annually.

Formal reviews are recommended every three years from the anniversary date of approval by the **Board**.

Recommendations for minor changes can be approved by **the Managing Director** before **the Board** review every three years.

Reference Code	AIUP/08/2026/V1.0
Executive Owner	The Managing Director
Policy Manager	The General Manager-Shared Services (AIMS Owner)
Effectiveness Approval Body	SBB Cambodia Board
Date Approved	18/09/2026
Effective Date	18/09/2026
Next Formal Review	18/09/2029
Version Number	V1.0
Jurisdictions	Cambodia, EU (Ireland), UK, Australia

ANNEX A. AI RISK ASSESSMENT FRAMEWORK

Every proposed AI use case is classified into one of the four risk tiers below before procurement, pilot or live use. The tier determines the controls that must be in place. Classification is recorded in the AI Usage Register and revisited at the review cadence in step 9 of the workflow.

A.1 Risk tiers and controls

Risk tier	Definition / typical SBB examples	Required controls
Unacceptable	Use case falls within Article 5 of the EU AI Act (see Section 5A). Examples: emotion recognition in our Cambodian classrooms; social scoring of donors; manipulative chatbots aimed at vulnerable supporters.	Prohibited. Refuse, do not procure, do not pilot. Document the refusal in the AI Usage Register.
High	Use case is or supports a system listed in EU AI Act Annex III (e.g. employment / recruitment screening, education access decisions, evaluation of access to essential services, credit-worthiness, biometric identification, critical infrastructure). For SBB this is rare but could apply if AI is used to short-list staff or to allocate scholarships/places.	AIMS Owner approval mandatory. Run a Fundamental Rights Impact Assessment (FRIA) and a DPIA. Implement human oversight (Article 14), input data quality controls, logging, and a documented human review of every individual decision. Register in AI Usage Register. Notify any serious incident to the relevant national competent authority within 15 days.
Limited	Use case is subject to transparency obligations (chatbots, AI-generated text/images for the public, deepfakes).	Apply Section 6A disclosures. Human review and editorial sign-off before publication. Register in AI Usage Register.
Minimal	All other AI uses with low risk and no transparency trigger (e.g. internal drafting, summarising, brainstorming, code assistance, spell-checking).	Standard rules in Sections 3, 4, 5 and 6 apply. Register in AI Usage Register if the tool is procured at organisational level. Personal-use accounts not permitted (Section 7).

A.2 Assessment workflow

The AI Responsible Person leads the following nine steps workflow for any new AI use case. The output is a one page record stored in the AI Usage Register.

1. Identify the proposed AI use case in plain English, including the AI tool, the input data, the output, and the human(s) responsible.

2. Screen against Section 5A (Article 5) prohibitions. If any prohibition applies, stop. Do not proceed.
3. Screen against EU AI Act Annex III to determine whether the use case is high-risk. If yes, escalate to the **AIMS Owner** before procurement and prepare a FRIA and DPIA.
4. Assess transparency triggers under Section 6A (Article 50). If yes, design the disclosure now (label, language, accessibility).
5. Assess data protection: identify personal data categories, lawful basis (GDPR / UK GDPR / Privacy Act 1988 / Cambodian PDPL 2024), and any cross-border transfer issues. Run a DPIA where required.
6. Assess jurisdictional scope (Section 14). If outputs are used in or affect persons in the EU, apply the EU regime in addition.
7. Record the use case in the AI Usage Register (Section 9) with all the fields, including risk tier and provider/deployer role.
8. Define the human oversight arrangement (who reviews, on what cadence, with what authority to override or stop).
9. Set a review date proportionate to risk: 6 months for high-risk, 12 months for limited, 24 months for minimal.

The same workflow applies in every jurisdiction. Where local law adds obligations (Section 14), they are appended to the record at step 6 and reflected in the controls.