INTOSAI IDI
DEVELOPMENT INITIATIVE

IDI POLICY

GENERATIVE ARTIFICIAL INTELLIGENCE

Digital Tools – Data Flows – Responsible innovation

2026

DOCUMENT CONTROL

Version Details

1.	**Date Effective from**	1 June 2026
2.	**Process of Development and Approval**	The policy has been developed by Corporate Support. Comments have been obtained from all staff. Approval was accorded by the IDI Director General upon the recommendation of the Deputy Director General (CS).
3.	**Schedule of Maintenance**	Annual Review in 2027
4.	**Version being replaced**	New Policy
5.	**Available at**	Teams: All staff: IDI Policies

TABLE OF CONTENTS

A. WHY THIS POLICY

1. Generative artificial intelligence can be a powerful tool to support our work at IDI — helping us draft materials, analyse information, and improve productivity. However, like any powerful tool, it also comes with **real risks if used without care or awareness**.
2. Understanding this policy helps ensure that **AI supports IDI's mission rather than undermines it,** by clarifying which AI tools are approved for use at IDI and under what conditions.
3. First, **IDI remains fully responsible for its work**, even when AI tools are involved. Generative AI can produce inaccurate, incomplete, or misleading information, and it does not understand IDI's context, values, or obligations. This is why all AI-generated content must always be reviewed, validated, and approved by a human before it is used. The responsibility for decisions and outputs always stays with IDI staff — never with the AI.
4. Second, **protecting data and confidentiality is essential**. Many publicly available AI tools store, reuse, or process information in ways that are not compatible with IDI's obligations towards SAIs, donors, staff, partners and other stakeholders. Entering confidential, sensitive, or personal information into the wrong AI system can lead to data leaks, legal issues, and loss of trust. **For this reason, only approved AI tools may be used in this context**, and this policy explains which tools may be used and why restrictions exist — not to prevent innovation, but to maintain the confidentiality of IDI's information.
5. Third, **IDI's credibility and reputation depend on trust**. As an organisation working in sensitive governance and accountability contexts, IDI must ensure that its outputs are accurate, ethical, inclusive and transparent. Misuse of AI — even unintentionally — could damage IDI's reputation, relationships, and legitimacy. Understanding the policy helps staff avoid situations where AI use could compromise these core assets.
6. Finally, the policy is designed to **enable responsible, lawful and confident use of AI**, not to ban it. By setting clear rules and expectations, IDI allows staff to use approved AI tools safely, with confidence that their work remains compliant with IDI's values, Code of Ethics, and accountability requirements. Informed use of AI helps IDI innovate while remaining trustworthy and responsible.

B. POLICY STATEMENT

7. Generative artificial intelligence (Gen AI) may support IDI's work when used responsibly. This policy sets out the mandatory rules governing the use of generative AI to protect IDI's integrity, data, reputation, and accountability.

MANDATORY RULES

8. These rules apply to all IDI staff and any individuals working on behalf of IDI.

   a. IDI staff must ensure that all AI-generated outputs are reviewed, validated, and remain under full human responsibility before use.

   b. IDI staff must protect confidential, sensitive, personal, and partner-provided information by using only IDI-approved AI tools where such data is involved.

   c. IDI staff must not use IDI email addresses or credentials to register for or access non IDI-approved tools, and the use of IDI telephone numbers for such purposes should be avoided unless strictly necessary (e.g. for identity verification or multi-factor authentication).

   d. IDI staff must ensure that all use of generative AI complies with IDI's Code of Ethics and all other applicable IDI policies.

   e. IDI staff must seek advice from the Internal IT Function (it@idi.no) when guidance or support is required for the appropriate use, testing, or implementation of generative AI tools.

9. All IDI staff have a duty to promptly report any breach of this AI Policy that they have committed, whether intentional or unintentional, to their line manager and the IT Function. Staff are also required to report any observed or suspected misuse of AI, non-compliance with applicable policies or legal requirements, or any unethical or inappropriate use of AI systems by all parties acting on behalf of IDI.

10. IDI will ensure that appropriate training is provided to all staff on the responsible, safe, and compliant use of Artificial Intelligence.

C. GUIDANCE – BEST PRACTICES FOR RESPONSIBLE USE OF GENERATIVE AI

11. The following best practices support compliance with the IDI Policy on the Use of Generative Artificial Intelligence. They provide practical guidance on how to use generative AI responsibly and safely in daily work. These practices do **not** create additional policy obligations.

12. **Preventing Data Leaks and Security Incidents**

    IDI staff should:

- Avoid using IDI credentials, institutional email addresses, or telephone numbers to register for or log in to publicly available generative AI applications.
- Avoid implementing or using code generated by generative AI in IDI systems without prior review and validation by IT specialist.
- Ensure that where technical testing is required, pilot environments or sandbox systems are used rather than live production systems.

13. **Protecting the Confidentiality of Sensitive Information**

    Users should:

- Avoid entering internal IDI information into generative AI applications that are not formally approved by IDI.
- Avoid entering personal data relating to staff members, partners, beneficiaries, or other third parties into non-approved generative AI tools.
- Apply the principle of data minimisation and only provide information that is strictly necessary for the task when using non-approved generative AI tools.

14. **Avoiding Intellectual Property and copyright Risks and Ensuring Transparency**

    Users should:

- Avoid using AI-generated outputs (including texts, graphics, videos) in institutional documents where there is a risk that the content may be protected by copyright or other intellectual property rights.
- Where appropriate, and without affecting the author's responsibility, clearly indicate when content has been generated or supported by generative AI.

15. **Preventing Bias, Harm, and Reputational Risk**

    Users should:

- Analyse AI-generated outputs to ensure they meet IDI's standards of legality,

fairness, ethics, inclusion and appropriateness.

- Review content carefully to ensure it does not contain discriminatory, biased, or harmful material.
- Always critically review and validate AI-generated outputs, even when the tool appears reliable or confident.
- Reflect honestly on their own ability to detect errors or inaccuracies before relying on AI-generated content.

16. **Respecting Intellectual Property and Third-Party Rights**

Users should:

- Avoid adopting, reusing, or reformulating AI-generated outputs where there is a reasonable suspicion that the content infringes the rights of third parties.
- Exercise caution when using AI outputs for external-facing or publishable materials.

17. **Implementation and Introduction of Generative AI Tools to Support IDI[1] Delivery[2]**

Users and teams should:

- Engage the Internal IT Function early when considering the introduction, configuration, or deployment of new generative AI tools or AI-supported automation for IDI work.
- Assess, with support from Internal IT where appropriate, the purpose of the tool, the associated risks, and its alignment with IDI's security, data-protection, and governance requirements.
- Ensure that new AI tools or automated processes are tested in controlled environments before any broader use.
- Pay particular attention to scenarios where AI is embedded into workflows or systems and where human review or intervention may be limited.
- Document assumptions, limitations, and safeguards for AI-enabled processes, especially where outputs may influence operational, analytical, or external-facing activities.

[2] I.e. Integrating AI into core delivery systems to support IDI's work, such as training AI to handle translation, produce training material, draft funding proposals, develop auditing guidance.

Annex 1 - Terms commonly used in AI

Term	Definition
Generative Artificial Intelligence (Generative AI)	Generative Artificial Intelligence (Generative AI) refers to a category of artificial intelligence systems capable of creating new content in response to user instructions. Such content may include text, audio, images, video, data analysis, or computer code. These systems generate outputs by learning patterns from large datasets and producing new material that resembles the data on which they were trained. Artificial intelligence more broadly encompasses technologies designed to perform tasks that typically require human intelligence, such as prediction, classification, pattern recognition, decision support, and automation. This Policy focuses on Generative AI because these systems interact directly with users and produce new content that may influence decisions, communications, or official outputs, presenting specific risks including inaccurate information, data disclosure, intellectual property concerns, and uncertainty regarding output reliability.
Large Language Model (LLM)	A Large Language Model (LLM) is a large-scale artificial neural network trained on extensive textual datasets to understand and generate natural language. LLMs identify statistical patterns in language and generate human-like responses but do not possess human reasoning or factual understanding and may generate inaccurate or fabricated outputs.
Hallucination	Hallucination refers to a phenomenon in which a generative AI system produces fictitious, fabricated, or factually incorrect content that appears coherent, plausible, and authoritative, and may be mistakenly accepted as accurate without appropriate human review and validation.
Prompt	A prompt is a written instruction, command, or query provided to a generative AI system to generate a response or perform a specific task. The quality, accuracy, and reliability of outputs may vary depending on the clarity and precision of the prompt.
Model Bias	Model bias refers to systematic tendencies embedded in the data used to train generative AI systems that may influence outputs, potentially resulting in unbalanced, discriminatory, or misleading

Term	Definition
	content.
Automation Bias	Automation bias is the tendency to place excessive trust in the outputs or recommendations of automated systems, sometimes at the expense of independent judgement and critical analysis.
Approved Generative AI Solutions	Approved generative AI solutions are AI tools formally authorised by IDI for use in IDI-related work. Such tools must meet IDI requirements relating to information security, data protection, confidentiality, governance, and contractual safeguards.
External Generative AI Platforms	External generative AI platforms are generative AI tools provided by third parties that are not formally approved by IDI. Examples include publicly available AI services such as ChatGPT, Claude and Gemini. These platforms may operate under data-handling practices and contractual terms that differ from IDI's internal governance standards and therefore require particular caution.
Internal IT Function	The Internal IT Function refers to the organisational unit within IDI responsible for the provision, operation, management, governance, and maintenance of digital infrastructure, IT systems, and technology services. The Internal IT Function supports and oversees the approval, monitoring, and governance of generative AI solutions used within IDI.

Annex 2 – Approved GenAI Solutions

This Annex complements the *IDI Policy on the Use of Generative Artificial Intelligence* and identifies the generative AI solutions that are formally approved for use within IDI **at the time of publication**.

Approved Solution

The following **generative AI solutions have been tested and approved for use within IDI**:

AI Solution		Approver
Microsoft Copilot, as provided through the **IDI Microsoft 365 tenant**[3]	April 2026	DDG Corporate support

Maintenance of the Annex

The list of approved Generative AI solutions may evolve over time to reflect technological developments, organisational needs, and governance decisions.

Updates to this Annex may be made without requiring a revision of the Policy itself.

[3] Microsoft Copilot operates within IDI's enterprise Microsoft 365 environment and is subject to IDI's information security, data-protection, confidentiality, and governance controls.

INTOSAI DEVELOPMENT INITIATIVE (IDI)
Stenersgata 2 | N-0184 Oslo | Norway
www.idi.no