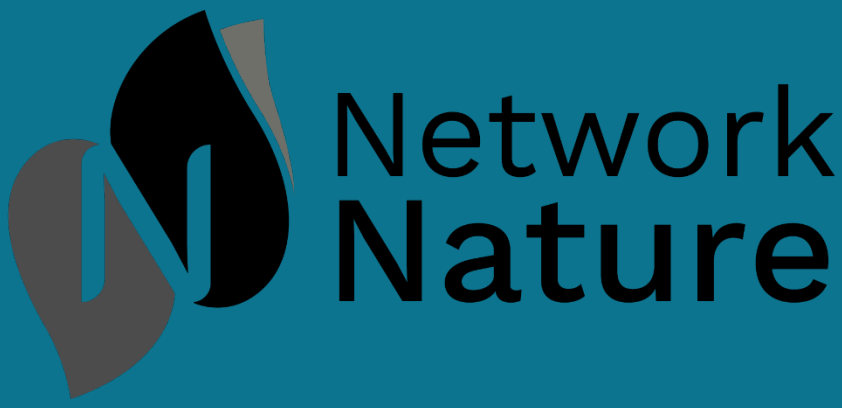

Task Force 1 Briefing Note:
Responsible use of AI by nature-based solutions projects

Responsible use of AI by nature-based solutions projects

Practical guidance for EU-funded NbS project managers and teams

NetworkNature Task Force 1 | briefing note | 2025

Key takeaway: *AI can help NbS projects work more efficiently and make better use of complex information. It should support - not replace - scientific judgement, local knowledge, stakeholder participation or human decisions. The project remains responsible for every output and decision, whether AI was used or not.*

Contents

Purpose and scope

This briefing is an output of the Task Force 1 Hackathon event in 2025, during which task force members explored recommendations for responsible use of artificial intelligence (AI) by EU-funded projects. Its purpose is to provide a practical starting point for nature-based solutions (NbS) projects considering the use of AI.

The briefing covers everyday generative AI tools as well as more specialised applications, such as habitat and species recognition, remote-sensing analysis, predictive modelling, knowledge extraction and decision-support systems. It draws on discussion within NetworkNature Task Force 1 (TF1) including concerns about bias, environmental impacts, unreliable outputs, confidentiality, transparency and the risk of allowing AI to displace human expertise.

Hackathon participants also identified useful applications: translating policy language, structuring and summarising information, generating ideas, recording project knowledge, identifying gaps and supporting data verification. The advice below develops those points into a proportionate process that projects can apply in practice.

This is practical guidance, not legal advice. Projects should also follow their grant agreement, organisational policies, research ethics procedures, data-management plan and any instructions from the European Commission or relevant funder.

Seven principles for responsible use

1. **Start with the need, not the technology**. Use AI only where it offers a clear benefit over a simpler method. Consider the full cost, including staff time, checking, procurement, energy and environmental impact.

2. **Keep people responsible and in control.** Name a human owner for the task. AI may inform a decision, but it should not make consequential decisions about people, places, funding, research quality or NbS priorities without meaningful human review.

3. **Protect people, communities and sensitive information.** Do not enter personal, confidential, commercially sensitive or unpublished material into a public AI service unless its use has been explicitly approved and appropriate safeguards are in place.

4. **Use evidence that is fit for the NbS context.** Check whether training and reference data represent the relevant ecosystems, seasons, geographies, languages and communities. A model that performs well elsewhere may fail in a local landscape or data-poor setting.

5. **Check outputs against authoritative sources and expert knowledge.** Treat AI-generated text, classifications, maps and recommendations as unverified until reviewed. Never rely on invented citations, confident wording or apparent numerical precision as proof of accuracy.

6. **Be open about significant use of AI.** Record and disclose AI use when it materially affects methods, analysis, findings, recommendations, public content or deliverables. Make it clear what the tool did and what people checked or changed.

7. **Learn and adapt.** Monitor performance, complaints, unintended effects and changing legal requirements. Stop or redesign an application if the risks outweigh the benefits.

A practical process for project teams

Use the following steps before introducing a new AI tool or applying AI to a new task. The depth of review should match the level of risk.

- **Define the task and intended benefit.** Describe the problem, users, expected output and why AI is being considered. Identify a non-AI alternative. For example: using image recognition to help screen thousands of camera-trap images may be justified; using a chatbot to draft a short email may not require a formal review.

- **Identify who and what could be affected.** Consider project staff, research participants, land managers, communities, rights-holders, species and ecosystems. Ask who might be excluded or misrepresented, and what would happen if the AI system was wrong.

- **Classify the risk.** Low-risk uses include brainstorming, language polishing and administrative summaries of non-sensitive material. Higher-risk uses include ecological classification, predictions, stakeholder profiling, automated recommendations, public-facing chatbots, or any use of personal, confidential, culturally sensitive or location-sensitive data.

- **Check the tool and its terms.** Confirm where data are stored, whether prompts or uploads are retained or used for training, who can access them, the model version, security arrangements, copyright terms, and whether the supplier offers an enterprise or governed environment. Do not assume that a paid account automatically makes a tool suitable.

- **Assess data and evidence.** Document the source, licence, quality, coverage and limitations of data. For NbS applications, check geographic and taxonomic coverage, seasonal variation, scale, resolution, class imbalance and whether local or traditional knowledge has been represented with permission and proper governance.

- **Plan human oversight and validation.** Agree who will check outputs, against what evidence, and what level of error is acceptable. Test on representative local data before deployment. For important applications, use independent review and compare results with established methods.

- **Record, communicate and monitor.** Keep a simple register of approved uses, tools, data, risk level, review decisions, validation results and responsible owners. Tell users when AI is involved, provide a route to question or correct outputs, and review the use periodically.

Risk levels: what proportionate review looks like

Level	Typical NbS examples	Minimum controls	Approval
Low	Brainstorming; editing non-sensitive text; translation checked by a fluent speaker; summarising public documents.	No sensitive data; human review; verify factual claims and sources; follow project disclosure rules.	Task owner
Medium	Extracting information from project documents; AI-assisted meeting notes; coding support; public-facing content; preliminary gap analysis.	Document tool and purpose; confirm data handling; test outputs; disclose material use; obtain consent for recording or transcription.	WP/task lead
High	Species or habitat classification; remote-sensing interpretation; predictive models; decision support; stakeholder profiling; processing personal, confidential, indigenous/ local or sensitive species data.	Formal risk and data-protection/ethics review; expert validation on local data; strong security; bias and impact testing; monitoring and appeal/ correction route.	Project governance plus relevant ethics/ DPO/ legal expertise
Do not use / redesign	Autonomous final decisions; replacing peer review or proposal evaluation; uploading confidential proposals or unpublished third-party work to public tools; fabricating or altering evidence; covert surveillance or manipulation.	Use a different process. Seek specialist advice where the proposed application may be prohibited or regulated.	Project coordinator / institution

Issues that need particular attention in NbS projects

Ecological and spatial bias: Many models and datasets are strongest for well-studied species, regions and languages. Performance may be weaker in biodiverse, rural or data-poor areas. Validate locally and report uncertainty rather than presenting a single answer as fact.

False precision and changing conditions: Ecological systems are dynamic. Predictions can be affected by weather, season, land-use change and differences in monitoring methods. Avoid turning uncertain outputs into exact-looking scores or maps without explaining confidence and limitations.

Local and traditional knowledge: AI must not be used to extract, combine or republish indigenous, traditional or community knowledge without appropriate permission, attribution and governance. Engage knowledge-holders directly; do not treat an AI-generated summary as a substitute for participation.

Sensitive locations and species: Exact locations of threatened species, nesting sites or vulnerable habitats can create risks if exposed. Apply data minimisation, access controls and appropriate spatial generalisation before using external tools or publishing outputs.

Stakeholder participation and fairness: Automated translation, sentiment analysis or stakeholder segmentation may overlook context, dialect, disability, digital exclusion or unequal power. Use these tools to support inclusive engagement, not to decide whose views count.

Environmental footprint: AI can support biodiversity monitoring and restoration, but it also consumes energy, water, hardware and staff resources. Choose the smallest suitable model and task, avoid unnecessary repeated generation, reuse verified outputs, and ask suppliers for credible environmental information where use is substantial.

Knowledge quality and project legacy: AI can help organise project knowledge, encode metadata and find links across outputs. Keep authoritative source files, clear authorship and durable metadata. Do not allow a chatbot or generated summary to become the only record of project evidence.

Using generative AI for common project tasks

Writing and communication. Useful for outlines, plain-language drafts and translation. A named person must check accuracy, tone, accessibility, cultural context, citations and compliance with EU visibility requirements. Do not publish generic AI text that obscures the people and evidence behind the work.

Meetings and workshops. Tell participants in advance if an AI note-taker, transcription or summarisation tool will be used. Confirm consent and data handling, particularly where discussions include personal data, unpublished results, commercially sensitive information or community knowledge. Check the summary against the recording or notes.

Literature and policy review. AI can help identify themes and search terms, but it can miss key sources, distort findings and invent references. Retrieve and read the original sources. Record the search method and do not present an AI-generated review as systematic or comprehensive unless it meets the relevant methodology.

Data analysis and coding. Use version control and reproducible workflows. Review generated code, test edge cases and document model versions and prompts where they materially affect results. Do not use synthetic data as if they were observed data.

Images, maps and design. Label synthetic or materially altered content where required and whenever audiences could be misled. Never use generated images as evidence of a site, species, intervention or project result. Retain provenance for maps, photographs and visualisations.

Proposals, deliverables and evaluation. Follow funder rules and disclose substantial use. AI can assist with structure and editing, but project partners remain responsible for originality, accuracy and commitments. Do not use public AI tools to evaluate confidential proposals, peer-review unpublished work or assess people.

Transparency: what should be disclosed?

Disclosure should be proportionate. Routine spelling correction may not need a statement. Use should normally be recorded and, where relevant, disclosed when AI materially shaped the method, interpretation, recommendations, public content or final output.

A useful disclosure answers four questions:

- Which tool and version was used?
- What task did it perform?
- What information or data was provided to it?
- How were the outputs checked, changed and approved by people?

Example statement: *"A generative AI tool was used to produce an initial thematic summary of publicly available project documents. The project team checked the summary against the source documents, corrected errors, added missing context and approved the final text. No personal, confidential or unpublished information was entered into the tool."*

A simple AI use register

A short register is often more useful than a long policy. It can sit alongside the project risk register, data-management plan or ethics procedures. Record at least:

- Task(s) in which AI is used and intended benefit
- AI tool, provider, version and date of use
- Responsible owner and approving person
- Data entered, its sensitivity and lawful/ethical basis
- Risk level and affected people, communities or ecosystems
- Validation method, known limitations and acceptable error
- Disclosure or labelling used
- Review date, incidents, complaints and corrective action

Quick checklist before you use AI

- ☐ Is there a clear purpose, and is AI better than a simpler option?
- ☐ Have we identified who or what could be harmed, excluded or misrepresented?
- ☐ Are the data lawful, ethical, representative and suitable for this ecosystem and location?
- ☐ Can we use the tool without exposing personal, confidential, unpublished or sensitive information?
- ☐ Do we understand the supplier’s data retention, training, security and copyright terms?
- ☐ Is a named person responsible for checking and approving the output?
- ☐ Have we tested accuracy, bias and limitations using representative local evidence?
- ☐ Will affected stakeholders be told, consulted or given a way to challenge the result?
- ☐ Have we recorded the use and planned any necessary disclosure or labelling?
- ☐ Is the expected benefit proportionate to the financial and environmental cost?

Governance and legal context

The EU Artificial Intelligence Act is now generally applicable, with phased dates for some high-risk systems. Its requirements depend on the system, its role and intended use. Projects should not assume that using a commercially available tool transfers responsibility to the supplier. AI literacy obligations also mean that organisations deploying AI should ensure staff have an appropriate level of knowledge and competence.

The General Data Protection Regulation (GDPR) continues to apply whenever personal data are processed. A Data Protection Impact Assessment may be required where processing is likely to create a high risk to people's rights and freedoms. Copyright, database rights, confidentiality, research integrity, cybersecurity, procurement and sector-specific rules may also apply.

Seek specialist advice early for high-risk or unfamiliar uses, especially where AI affects people's rights, evaluates individuals, processes sensitive data, uses biometric or surveillance functions, or becomes part of a tool offered to others.

Further reading

- European Commission - Updated ERA Living Guidelines on the responsible use of generative AI in research (2026)
- European Commission - EU Artificial Intelligence Act overview and implementation timeline
- European Commission - Ethics Guidelines for Trustworthy AI
- European Data Protection Board - Artificial intelligence and data protection resources
- UNESCO - Recommendation on the Ethics of Artificial Intelligence
- UNESCO - AI and the environment: practical implementation toolkit
- NIST - AI Risk Management Framework and Generative AI Profile
- NetworkNature - Websites in an AI-driven world

About this briefing

This briefing was developed through NetworkNature Task Force 1, a cross-project forum for people interested in data and knowledge sharing. It builds on a workshop held with Task Force members and has been expanded to reflect current European and international guidance. It should be treated as a living resource and reviewed as technology, evidence and regulation develop.

Contact: TF1@networknature.eu | networknature.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 887396 and from Horizon Europe under grant No 101082213.

UK Research and Innovation

This project is funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee.