



Artificial Intelligence Policy for Applicants and Grantees of the Biodiversity Challenge Funds

July 2026

Biodiversity Challenge Funds:

Darwin Initiative

Illegal Wildlife Trade Challenge Fund

Darwin Plus

1	Purpose of this Policy	2
2	Scope	2
3	Core Principles for Responsible AI Use	3
4	Data Protection, Ethics, Fairness, and Bias	5
5	Examples of Acceptable Uses of AI	5
6	Examples of Unacceptable Uses of AI	6
7	Requirements for Transparency and Accountability	6
8	Guidance for Grantees: Using AI During Project Delivery	7
9	Consequences of Non-Compliance	8
10	Support and Further Resources	8

1 Purpose of this Policy

Artificial Intelligence (AI) has high potential to improve the quality and clarity of applications and project outputs within the Biodiversity Challenge Funds (BCFs) including supporting non-native speakers to work in English, but its use also comes with significant risks if misused.

This policy sets expectations for how applicants and grantees may use AI when preparing BCFs applications and delivering BCFs-funded projects. There is no requirement or expectation that AI is used, but where it is used it is critical that best practice is followed to maintain ethical and quality standards.

Because AI is a general-purpose technology, the guidance included in this policy outlines our core principles for responsible use and should be used to develop your own bespoke way of using AI.

The purpose of this policy is to:

- Ensure accuracy, transparency, and integrity of information submitted to the Funds.
- Reduce risks related to misuse of AI, including privacy breaches, biased outputs, and fabricated information.
- Promote responsible, ethical, and secure usage of AI to improve quality and efficiency of work.

2 Scope

This policy applies to:

- All applicants preparing concept notes, applications, budgets, logframes, and supporting documentation for any BCF funding round.
- All grantees preparing project reports, financial claims, evidence submissions, and communications products.
- Any third parties preparing materials on behalf of applicants or grantees, for example partners or subcontractors.

It covers all generative AI tools (e.g., ChatGPT, Claude, Copilot), document-based AI assistants, translation tools, and AI-enabled data analysis systems.

3 Core Principles for Responsible AI Use

The following principles reflect BCFs' internal safe use guardrails and expectations for AI use.

3.1 AI should assist, not replace, human judgement

AI may be used to refine ideas, summarise nonconfidential content, or improve clarity but it must not be used to generate false, misleading, or invented information.

Applicants and grantees must:

- Maintain full ownership of all assessments, claims, and narratives.
- Use AI only to support thinking and drafting, not to automate decisions or fabricate (intentionally or unintentionally) evidence. AI outputs should never be copied verbatim into applications or reports,
- Ensure that staff remain engaged with all content and accountable for accuracy.

3.2 Authenticity and accuracy are mandatory

All text, data, evidence, and claims submitted to the BCFs must reflect genuine, real-world information:

- AI-generated content must never invent achievements, results, baselines, stakeholder engagement, impacts, or financial information.
- AI tools can introduce hallucinations; applicants and grantees must thoroughly review, fact-check, and evaluate all outputs by relevant human experts.
- Reviewers¹ may request clarification if AI-generated patterns or phrasing indicate potential inaccuracy, bias, or ambiguity.

¹ In the context of this document, the term reviewer refers to any individual or group responsible for examining, assessing, or clarifying information submitted to the BCFs at various stages and in different formats. This includes the following roles:

Expert group members: specialists who evaluate applications.

Report Reviewers: individuals who review progress reports, and other submitted documentation.

Administrative staff for other information: personnel who may review communications, financial information, change requests, or other documents that are not part of the formal application or reporting forms but are provided in the course of the grant or project lifecycle.

3.3 Protect confidentiality and personal data

It is important that all confidential and personal data is protected:

- Do not enter sensitive, unpublished, or confidential project information into public or insecure AI tools.
- Personal data must not be input into AI systems unless the tool is secure, compliant, and approved by your organisation.
- AI must not be used to process information that could put individuals or communities at risk.

3.4 Use secure and approved tools

Only use secure, vetted AI tools (e.g., paid or enterprise versions) and avoid free/open platforms for sensitive content.

Applicants and grantees should:

- Avoid free AI tools for any non-public project documentation or data.
- Follow their organisation's data protection, safeguarding, and IT security policies.
- Ensure tools comply with national data protection laws (e.g., UK GDPR², where applicable).

3.5 Transparency in use

Applicants and grantees must disclose in their documentation:

- Whether AI was used,
- Which tools were used, and
- The types of tasks AI supported (e.g. summarising public literature, structuring text).

AI use does not disadvantage applicants. However, undisclosed or inappropriate use may result in clarification requests or, in serious cases, ineligibility.

² The UK General Data Protection Regulation (UK GDPR) is a UK law that sets out the key principles, rights and obligations for most processing of personal data in the UK.

4 Data Protection, Ethics, Fairness, and Bias

BCFs internal studies highlight the risks of bias, cultural misinterpretation, and environmental impacts of AI use. Applicants and grantees must ensure:

- AI outputs are checked for potential bias, particularly in Gender Equality, Disability, and Social Inclusion (GEDSI)-related analysis and safeguarding.
- No AI tool is used to profile individuals or communities.
- AI use aligns with ethical standards and human rights principles.
- Use of computationally intensive AI is proportionate and environmentally responsible.

5 Examples of Acceptable Uses of AI

5.1 Application drafting and report writing support

- Helping articulate complex ideas that the applicant or project already understands.
- Producing first-draft text based solely on content the applicant or project provides.
- Drafting narrative sections based on project-generated evidence.
- Summarising monitoring data already compiled by the team.
- Summarising publicly available information.
- Improving readability and coherence of reports including clarity, grammar, and structure.

5.2 Project preparation and research

- Generating summaries of public datasets or literature (with accuracy checks).
- Helping brainstorm risks, assumptions, or theories of change, provided the applicant retains critical oversight.

5.2.1 Translation and language support

- AI-assisted translation for improved clarity, followed by human review.

6 Examples of Unacceptable Uses of AI

To avoid over-reliance and hallucinations, AI must not be used to:

6.1 Invent or fabricate

- Results, achievements, outputs, impacts, financial numbers, baselines, or stakeholder views.
- Evidence, citations, or case studies.

6.2 Complete assessments designed to test organisational capability

- Logframe design, monitoring, evaluation and learning (MEL) plans, safeguarding assessments, risk matrices, or financial analyses. These must reflect genuine project design and team expertise, not AI-generated content alone.

6.3 Conduct automated due diligence on affected people

- AI cannot be used to analyse community profiles, vulnerabilities, or GEDSI characteristics using scraped³ or unverified data.

6.4 Replace stakeholder engagement or consultation

- AI may help summarise meeting notes, but it cannot stand in for engagement or consultation with communities, partners, or authorities.

7 Requirements for Transparency and Accountability

7.1 Declaration of AI use

All applicants and grantees must first answer a short yes/no question in the application/reporting form:

Please indicate whether Artificial Intelligence (AI) tools were used in preparing this application.

If yes, check box to confirm that all outputs were verified and no sensitive data was entered into insecure tools:

☐ Yes

☐ No

³ To scrape (or data scraping/web scraping) is defined as the automated extraction and copying of data or content from websites, online platforms, databases, or other digital sources, typically without direct coordination with, or permission from, the data holder, for the purpose of analysis, reuse, or training artificial intelligence systems.

If yes, briefly describe:

- *Which and how AI tools were used, including for which tasks, at what stage, and for what purpose;*
- *How outputs were reviewed and verified to ensure accuracy and reliability.*

If you answer no, you do not need to provide any further information. If it is found that AI tools have been used without acknowledgement, then the application may be deemed to be ineligible.

This declaration does not apply to the use of basic tools, such as tools used to check grammar, spelling, and references.

7.2 Responsibility for accuracy

Applicants remain fully responsible for all submitted content.

Where AI errors are detected (e.g., invented facts, inconsistencies), the BCFs may request clarification, correction or, if significant, the application may be deemed ineligible.

If an applicant repeatedly or intentionally misuses AI tools, the fund manager will record this behaviour. Such actions could result in the applicant/grantee being disqualified from future application processes.

8 Guidance for Grantees: Using AI During Project Delivery

8.1 MEL and reporting

AI can be used to summarise monitoring data that has been manually entered by the project team, assist in structuring narrative reflections, lessons, and challenges, and support the drafting of sections of reports- provided that it only uses information supplied by the project and that the final information submitted is checked by the project team before submission.

AI must not be used to produce evidence that the project has not actually collected, generate its own scores or ratings, or independently scan sensitive documents unless the specific tool employed is secure and has received appropriate approval.

8.2 Risk management

Project teams are best placed to understand the risks specific to their work. While AI can support the identification of potential risks in written information, it is crucial that project teams use their own judgement to critically assess and verify those risks, ensuring accuracy and responsibility throughout.

AI must not be used to analyse personal or sensitive risk data unless appropriate safeguards are in place to protect such information.

8.3 Communications and outreach

AI tools may be used to assist in drafting materials intended for public dissemination; however, it is essential that all outputs are thoroughly checked for accuracy.

AI must not be used to generate images or content that could misrepresent the actual achievements of the project. AI tools must not be used to supply text, images, or data from non-project sources, except with clear citation/accreditation.

9 Consequences of Non-Compliance

Violations may result in:

- Ineligibility or non-compliance flags in grant management processes.
- For serious breaches (e.g., falsification), rejection of applications or grant termination.
- For repeat offences, this may result in disqualification from future BCFs funding.

10 Support and Further Resources

Applicants and grantees may contact the BCFs team for advice on appropriate AI use.

The UK Civil Service AI recruitment guidance (source of acceptable/unacceptable use framing) can be read here:

<https://www.civil-service-careers.gov.uk/artificial-intelligence-and-recruitment/>

The BCFs may publish additional examples of responsible AI use over time.