Policy for the Responsible Use of Artificial Intelligence

Version 1.0 (11 November 2026)

Table of Contents

01. Introduction and Purpose 1

02. Principles for Responsible AI Use 3

03. Risk-Based Approach to AI Use 4

04. For Applicants and Beneficiaries 6

05. For Reviewers and Evaluators 8

06. For IDEP Staff and Personnel 10

07. AI Transparency Requirements 12

08. Governance and Accountability 13

09. AI Approval and Procurement 14

10. Literacy and Skills Development 15

11. Incidents and Non-Compliance 16

Annex 1 — Operational Review Matrix 17

Annex 2 — Illustrative AI Use Cases 17

Annex 3 — Key Terms and Definitions 22

Annex 4 — Reference Framework 23

01. Introduction and Purpose

Policy Status and Scope

Artificial Intelligence (AI) is increasingly integrated into tools used for drafting, translation, information retrieval, analysis, communication, administration, and decision support. For the purposes of this Policy, AI includes relevant generative and non-generative AI functionality, including AI features embedded in commonly used software. When used responsibly, these tools can improve efficiency, accessibility, and the quality of work. Their inappropriate use, however, can introduce inaccuracies, bias, confidentiality risks, data protection concerns, and excessive reliance on automated outputs.

This Policy establishes the framework of the Foundation for the Management of European Lifelong Learning Programmes (IDEP) for the responsible use of AI in its operations and in the implementation of the Erasmus+ and European Solidarity Corps (ESC) programmes.

The Policy is binding on IDEP personnel. It also applies, where incorporated into applicable contracts, terms of engagement, instructions, or other arrangements, to external evaluators, contractors, service providers, and other persons acting on behalf of IDEP.

For applicants and beneficiaries, the principles in Section 2 and the provisions of Section 4 primarily provide guidance on responsible AI use in the context of Erasmus+ and ESC. They do not, by themselves, create additional eligibility, award, reporting, or contractual requirements unless such requirements arise from applicable legislation, Programme Guides, grant agreements, calls for proposals, or other binding programme provisions.

Relationship with EC Guidance

This Policy implements at IDEP level the principles and recommendations contained in the European Commission's *Guidelines on the Use of Artificial Intelligence in Erasmus+ and European Solidarity Corps Programmes*.

The Commission Guidelines provide the overarching programme framework. This Policy establishes the responsibilities, permissions, restrictions, safeguards, and governance arrangements applicable within IDEP's operational context.

The Policy should therefore be read together with the applicable Erasmus+ and ESC Programme Guides, European Commission guidance, relevant data protection requirements, and applicable EU and national legislation.

Where any provision of this Policy is inconsistent with binding legislation, the applicable Programme Guides, grant conditions, or binding instructions issued by the European Commission, those higher-level requirements shall prevail.

Why Responsible AI Use Matters

Responsible AI use can reduce administrative burden, support clearer communication, assist with analysis, and improve access to information. It can also help staff, applicants, beneficiaries, and evaluators work more efficiently.

These benefits depend on the way AI is used. AI-generated outputs may be inaccurate, incomplete, biased, overly generic, or misleading. AI systems may also process information in ways that are unsuitable for personal, confidential, or otherwise protected data.

Responsible use therefore requires a combination of human judgement, appropriate technology, data protection, transparency, verification, and safeguards proportionate to the potential impact of the use.

Policy Review and Updates

AI technologies, legal requirements, programme guidance, and operational practices continue to evolve. This Policy shall therefore be reviewed periodically and updated when necessary.

IDEP may also issue supporting instructions, information on approved tools and use cases, checklists, examples, or other operational guidance without requiring amendment of the Policy itself, provided that such materials remain consistent with it.

02. Principles for Responsible AI Use

The following seven principles apply across the uses covered by this Policy. These principles are reflected in the risk framework in Section 3 and operationalised in Sections 4–6 through five recurring operational areas for the three stakeholder groups.

Human Oversight and Responsibility

AI should support, not replace, accountable human judgement. Persons using AI remain responsible for the work they perform and for the outputs they adopt, submit, communicate, or rely upon.

Decisions of consequence must remain subject to meaningful human judgement. Responsibility cannot be transferred to an AI system.

Proportionality and Risk

The safeguards applied to AI use should reflect its purpose, context, and potential impact.

Routine uses such as language correction or formatting generally require fewer safeguards than uses involving confidential data, assessment, eligibility, funding decisions, or other matters affecting individuals or organisations.

AI tools and methods should also be proportionate to the task. Resource-intensive systems should not be used unnecessarily where simpler tools can adequately achieve the intended purpose.

Transparency and Explainability

AI use should be sufficiently transparent for IDEP to understand its role where this is relevant to accountability, assessment, compliance, or audit.

Higher-impact uses should be capable of being explained in practical terms, including the purpose for which AI was used, the information processed, the role of the AI output, and the human checks applied.

Transparency does not mean that every routine use of AI must be publicly disclosed. Disclosure and documentation requirements should be proportionate and must comply with applicable law and programme rules.

Fairness and Inclusivity

AI systems may reproduce or amplify biases and may omit important context or nuance.

Users should consider whether AI-supported outputs could disadvantage particular persons, organisations, regions, languages, project types, or groups. Particular care is required where AI supports assessment, prioritisation, analysis, or communication affecting access to programme opportunities.

Privacy, Confidentiality, and Security

AI use must comply with applicable data protection, confidentiality, information-security, and professional obligations.

Personal, confidential, or non-public information must not be entered into AI systems unless the system and specific use are authorised or otherwise allowed for the relevant type of information and appropriate safeguards are in place.

Accuracy and Reliability

AI-generated information must not be assumed to be correct.

Users must apply an appropriate level of verification, particularly for factual statements, figures, dates, legal or programme references, quotations, citations, translations, summaries, and information that may influence official action.

Verification should rely on authoritative or otherwise appropriate sources rather than on repeated questioning of the AI system alone.

Originality and Intellectual Property

AI use must respect applicable intellectual property rights, authorship requirements, and programme rules concerning original content.

AI must not be used to fabricate sources, disguise plagiarism, misrepresent the origin of work, or present unverified generated material as fact.

03. Risk-Based Approach to AI Use

IDEP applies a risk-based and context-sensitive approach to AI use.

Operational Review Tiers

The operational review tiers characterise the nature and risk profile of a particular AI use and indicate the level of scrutiny, oversight, and safeguards appropriate to it, taking account of its purpose, context, information processed, the role assigned to AI, and potential impact.

For the purposes of this Policy, AI uses fall within one of the following operational review tiers. Whether a required approval, authorised tool, institutional arrangement, or other safeguard has been established does not alter the operational tier of the use.

Tier 1 — Routine, where the AI use is administrative or supportive, does not materially influence programme outcomes or individual rights, and does not involve protected information. Examples may include grammar correction, formatting, or drafting non-sensitive internal correspondence.

Tier 2 — Elevated, where AI processes substantive information or supports work that may influence an official output but does not itself play a consequential or decisive role and remains subject to direct human review. Examples may include substantive summarisation, translation of substantive material, analysis of appropriately prepared programme information, or identification of inconsistencies.

Tier 3 — Intensive, where AI use may materially affect eligibility, scoring, ranking, funding, rights, complaints, or other consequential decisions, or involves protected information in a manner requiring enhanced institutional controls. Such uses require enhanced scrutiny, safeguards, and documentation.

Tier 4 — Critical, where the intended AI use would create risks to accountability, fairness, confidentiality, programme integrity, or compliance that cannot be adequately mitigated within that use. Such uses are prohibited under this Policy.

These operational tiers are internal to IDEP and do not constitute or replace the legal classifications established by the EU Artificial Intelligence Act.

Policy Use Determination

A particular AI use may have one of the following determinations under this Policy:

Permitted — the use may be undertaken where the applicable requirements can be satisfied directly by the stakeholder, without an additional authorisation, institutional arrangement, or other prerequisite outside their direct control.

Conditional — the use may be undertaken only where an additional authorisation, approved tool or use case, institutional arrangement, or other prerequisite outside the stakeholder's direct control is in place.

Prohibited — the use must not be undertaken and may not be authorised under this Policy.

Permitted does not mean unconditional: all applicable requirements of this Policy continue to apply. A Conditional use remains Conditional after the relevant prerequisite has been satisfied; satisfaction of that prerequisite determines whether a particular instance of the use may proceed.

For IDEP personnel, and for persons acting on behalf of IDEP where this Policy forms part of their applicable terms or instructions, a Policy Use Determination has operative effect under this Policy. For applicants and beneficiaries, the determination expresses IDEP's guidance on responsible AI use and does not, by itself, create a permission, prohibition, eligibility condition, or other binding programme requirement. Any binding requirement applicable to applicants or beneficiaries derives from applicable legislation, Programme Guides, calls for proposals, grant agreements, their institutional requirements, or other binding provisions.

Approved Tools and Use Cases

IDEP shall maintain a **Register of Approved AI Tools and Use Cases**.

The Register identifies, as appropriate:

- the AI tool or system;
- the purposes for which it is approved;
- the applicable operational review tier;
- the applicable policy use determination;
- the categories of information that may be processed;
- relevant restrictions or conditions;
- any required human review, documentation, or training.

Approval of a tool for one purpose does not imply approval for all purposes or data categories. Inclusion in the Register constitutes IDEP authorisation for the specified use and does not imply endorsement or approval by the European Commission.

IDEP shall make relevant information from the Register readily accessible to personnel and shall inform evaluators, contractors, and other persons acting on its behalf of the approved tools and conditions applicable to their roles.

Unless and until an AI tool has been expressly approved for processing confidential application or report content, such content must not be entered into that AI system.

04. For Applicants and Beneficiaries

Applicants and beneficiaries remain responsible for the quality, accuracy, originality, and compliance of the materials they submit or produce.

Use of AI is not, in itself, a positive or negative factor in the assessment of an application, report, or project output. The relevant programme requirements and assessment criteria continue to apply regardless of whether AI has been used.

Using AI Appropriately and Proportionately

Applicants and beneficiaries may use AI tools to support activities such as brainstorming, structuring ideas, language improvement, translation, formatting, research assistance, drafting, data visualisation, and preparation of project materials.

The extent of AI use should remain appropriate to the task. AI may support the development or expression of ideas, but the final material should accurately represent the applicant's or beneficiary's actual project, intentions, activities, results, and circumstances.

Applicants and beneficiaries should avoid excessive reliance on generic AI-generated material or using AI in ways that conceal a lack of genuine engagement with the project.

Retaining Human Oversight and Responsibility

AI should support, not replace, the applicant's or beneficiary's own judgement.

AI-generated material must be reviewed before it is submitted, published, or otherwise relied upon. Applicants and beneficiaries remain fully responsible for the content they submit and cannot transfer responsibility for inaccuracies, omissions, or misrepresentations to the AI tool used.

Checking Accuracy, Fairness, and Originality

Applicants and beneficiaries must assess whether AI-generated material is accurate, relevant, specific, and consistent with the project concerned.

AI may generate unsupported claims, invented references, incorrect programme information, generic project descriptions, or unrealistic activities. Factual claims and sources should therefore be verified using appropriate and reliable information.

Applicants and beneficiaries should also consider whether AI-generated suggestions or content introduce bias, exclude relevant perspectives, or misrepresent the social, cultural, organisational, or local context of the project.

Submitted content must comply with applicable requirements concerning originality, authorship, plagiarism, and intellectual property. AI must not be used to fabricate project activities, partnerships, experience, statistics, results, evidence, references, or other information.

Where deficiencies affect the applicable assessment criteria, they may affect the assessment in the same way as equivalent deficiencies in material produced without AI. Suspected AI use should not, by itself, be treated as evidence of poor quality or non-compliance.

Protecting Data, Confidentiality, and Security

Applicants and beneficiaries should avoid sharing personal data, particularly sensitive or directly identifying information, with AI tools unless they are satisfied that the processing is lawful and appropriately protected.

Particular care should be taken with information concerning participants, partners, CVs, identification details, contact information, health or accessibility information, and non-public project documentation.

Organisations should use institutionally authorised tools where required by their own internal rules and should apply appropriate data minimisation and security safeguards.

Ensuring Transparency and Documentation

Applicants and beneficiaries must comply with any disclosure or documentation obligation concerning AI use arising from applicable legislation, the relevant Programme Guide, a call for proposals, a grant agreement, or another binding programme provision. This Policy does not impose any additional general disclosure requirement beyond those applicable requirements.

Where clarification concerning relevant AI use is formally requested in accordance with applicable programme procedures, applicants and beneficiaries should provide accurate information. They should also be able to explain, in general terms, relevant AI use where this is material to verification, compliance, or a formal request.

05. For Reviewers and Evaluators

Reviewers and evaluators safeguard the fairness, independence, confidentiality, and quality of the assessment process.

AI may assist allowed aspects of their work but must not replace expert judgement or undermine the requirement to assess applications, reports, and outputs against the applicable programme criteria.

Using AI Appropriately and Proportionately

AI may be used for supportive and non-decisive tasks consistent with this Policy. Routine uses that do not process application, report, assessment, or other protected information and do not influence the substance of an assessment may be undertaken without separate prior IDEP authorisation. Other uses are subject to the safeguards applicable under this Policy.

Potential uses may include organising notes, refining language, assisting with information retrieval, summarising material, identifying inconsistencies, or supporting the drafting of feedback.

The extent of AI assistance and the safeguards applied should be proportionate to the sensitivity and potential impact of the task. Uses connected more closely with eligibility, scoring, substantive assessment, or confidential information require greater scrutiny than routine language or organisational assistance and may also require IDEP authorisation.

Where AI is used to summarise or analyse application or report content, the evaluator must still review the source material to the extent required for a proper assessment.

Retaining Human Oversight and Responsibility

Evaluators must not delegate their substantive judgement to AI.

AI must not determine the final score, make the final eligibility determination, rank applications for funding, substitute for the evaluator's assessment of the relevant criteria, or produce an evaluation that the evaluator adopts without independent consideration. AI use must not reduce or circumvent any procedural safeguards, review rights, or other protections available under applicable programme rules or law.

Evaluators remain personally responsible for the assessments they submit. Any AI-assisted output must be independently reviewed and validated before it contributes to assessment work.

Checking Accuracy, Fairness, and Originality

Evaluators must consider the complete and relevant context of the application or report and apply the applicable programme criteria using their own expertise.

AI-assisted summaries, analyses, or draft feedback should be checked for factual accuracy, omitted information, inappropriate emphasis, bias, and loss of important context or nuance.

AI-assisted feedback must accurately reflect the evaluator's own assessment and scoring rationale and be specific to the application concerned. Templated or generic wording should be avoided.

Where originality, authorship, plagiarism, or intellectual property are relevant under the applicable programme rules or assessment criteria, evaluators should assess these matters on the basis of the applicable requirements and available evidence. Suspected AI use should not itself be treated as proof of plagiarism, lack of originality, or poor quality.

Where there are specific grounds to suspect plagiarism, fabrication, or another breach of applicable programme requirements, evaluators should follow the relevant IDEP or programme procedure rather than attempt to determine the matter solely through AI-detection tools.

AI-detection tools should not be treated as conclusive evidence that content was generated by AI. Where material appears generic, inconsistent, inaccurate, or insufficiently specific, evaluators should assess the substantive deficiency against the relevant programme criteria. Where suspected AI influence is relevant to a substantive deficiency or possible non-compliance, any internal observation should be recorded factually and linked to the applicable programme requirement or assessment criterion.

Protecting Data, Confidentiality, and Security

Applications, reports, supporting documents, and assessment information may contain confidential, personal, or otherwise non-public information.

Evaluators must not enter, upload, reproduce, or otherwise process such information through unapproved AI systems.

AI processing of application or report content may take place only where IDEP has approved the relevant system and use case and confirmed that applicable confidentiality, security, and data protection requirements are satisfied.

Until such an authorised arrangement exists, the absence of an approved system means that evaluators must not use AI tools to process application or report content.

Ensuring Transparency and Documentation

Where an evaluator uses AI in an authorised manner in connection with substantive assessment work, the use must be documented in accordance with IDEP requirements.

Documentation may include the purpose and scope of the AI use, the approved tool used, and the manner in which the output was reviewed or validated.

Routine AI assistance that does not process application or report content and does not influence the substance of the assessment need not be documented unless IDEP instructions provide otherwise.

Any additional transparency or documentation requirement arising from applicable legislation, programme rules, contractual terms, or IDEP instructions must be respected.

06. For IDEP Staff and Personnel

IDEP personnel are expected to model responsible AI use in programme management, administration, communication, and institutional work.

AI may be used to improve efficiency and quality where its use is appropriate to the task and consistent with this Policy.

Using AI Appropriately and Proportionately

Personnel may undertake AI uses in accordance with any conditions established for the relevant tool or use case.

Examples may include drafting or improving correspondence, preparing outlines, summarising non-sensitive material, translating content, organising information, preparing public communications, assisting with spreadsheets or code, identifying patterns in appropriately prepared data, transcribing or summarising meetings, and preparing action points.

Uses connected with eligibility, assessment, complaints, procurement, recruitment, grant management, ranking, fraud or irregularity detection, or other decisions affecting persons or organisations require greater scrutiny and may only be undertaken where the relevant use case has been authorised and the required safeguards have been established.

AI may assist with clearly defined preparatory or administrative aspects of such processes, such as identifying missing fields or flagging inconsistencies, but the level of AI involvement must remain proportionate to the potential impact of the task.

Retaining Human Oversight and Responsibility

IDEP personnel remain responsible for outputs they use in their work.

AI must not be treated as the sole or decisive basis for an official determination concerning eligibility, funding, assessment, complaints, recruitment, procurement, or other consequential matters.

AI-generated material intended for official decisions, formal communications, guidance, reports, publications, legal or programme interpretations, or other consequential purposes must receive a level of human review proportionate to its importance.

Responsibility for the final output or decision remains with the responsible IDEP personnel or authorised decision-maker and cannot be transferred to the AI system.

Checking Accuracy, Fairness, and Originality

AI-generated information must not be assumed to be correct merely because it appears plausible or well presented.

Factual statements, sources, legal provisions, programme requirements, figures, translations, and other material capable of affecting stakeholders must be independently verified where appropriate.

Personnel should also consider whether AI-assisted analysis, recommendations, or communications could introduce or reinforce bias, disadvantage particular persons or organisations, omit important contextual factors, or undermine IDEP's commitments to fairness and inclusion.

AI-assisted outputs used by IDEP must respect applicable intellectual property and authorship requirements. AI must not be used to fabricate information, sources, evidence, or institutional records, or to reproduce or present third-party material inappropriately.

Protecting Data, Confidentiality, and Security

Personnel must not enter personal, confidential, application-related, commercially sensitive, security-related, or other protected information into unapproved AI tools.

Where an approved tool is available, information may only be processed within the purposes and data categories for which that tool has been authorised.

Where appropriate, anonymisation, data minimisation, access restrictions, retention controls, and settings preventing reuse of IDEP information for model training should be considered as part of the approval and use process.

Where AI is used to record, transcribe, or summarise meetings, personnel must ensure that the tool is authorised for the information concerned and that applicable requirements concerning participant notification, data protection, confidentiality, and retention are respected.

Ensuring Transparency and Documentation

Ordinary use of AI for drafting, language improvement, formatting, brainstorming, or similar support does not require routine public disclosure merely because AI was involved.

Where applicable law or programme rules require disclosure of AI use or AI-generated content, those requirements must be respected.

Internal documentation is required where AI processes protected information, contributes to assessment or decision-support workflows, or is relevant to accountability or auditability.

Personnel must comply with any recording, approval, or documentation requirements established for the relevant AI tool or use case.

07. AI Transparency Requirements

IDEP shall comply with applicable legal transparency obligations when deploying AI systems or publishing AI-generated or manipulated content.

The requirement for transparency depends on the system, content, context, and applicable legislation. It is therefore distinct from a general expectation that every AI-assisted output should carry an AI label.

Without limiting any broader legal obligation, particular attention should be given to the following situations:

Direct Interaction with AI

Where IDEP deploys an AI system that interacts directly with individuals, such as an AI chatbot or comparable interactive service, IDEP shall ensure that users are informed that they are interacting with AI where required by applicable law.

Deepfake and Manipulated Media

Where IDEP uses AI-generated or manipulated image, audio, or video content that falls within applicable legal rules concerning deepfakes or comparable synthetic media, the required disclosure shall be made clearly and appropriately.

AI-Generated Public-Interest Text

AI-generated or manipulated text published for the purpose of informing the public on matters of public interest shall be labelled where required by applicable law.

Where applicable law provides an exception to the requirement to inform the public, for example where AI-generated or manipulated text has undergone human review or editorial control and is subject to editorial responsibility, IDEP may rely on that exception only where the review is genuine and substantive rather than merely formal.

Other Regulated Uses of AI

Where IDEP deploys AI systems subject to specific transparency obligations, the applicable information and disclosure requirements must be respected. Nothing in this Policy authorises an AI use that is prohibited or otherwise restricted under applicable law.

The examples above are not exhaustive. IDEP shall review transparency requirements when approving new AI systems or materially new use cases.

08. Governance and Accountability

Responsible AI use requires both individual care and institutional safeguards.

Management Responsibility

IDEP Management retains overall responsibility for the organisational implementation of this Policy and for determining the level of authorisation required for higher-risk uses.

Policy Coordination

IDEP has a designated function to coordinate implementation of this Policy under the role of the Officer for Horizontal Priorities.

The designated function should, as appropriate:

- coordinate periodic review of the Policy;
- maintain the Register of Approved AI Tools and Use Cases;
- support consistent interpretation of the Policy;
- coordinate relevant guidance and training;
- facilitate review of proposed higher-risk AI uses;
- support monitoring of significant developments in EU and programme guidance.

The Policy does not require the creation of a separate AI committee. IDEP may allocate these responsibilities within its existing structures.

Data Protection and Security

The Data Protection Officer or other appropriate data protection function shall be consulted where proposed AI use involves personal data or raises material data protection considerations.

The appropriate IT or information-security function shall assess relevant security, access, data-handling, retention, integration, and technical risks before an AI tool is approved for protected information or institutional deployment.

Process Ownership

Each significant institutional AI use case shall have an identifiable process or business owner responsible for ensuring that the system is used for its approved purpose and that required safeguards remain operational.

AI Use-Case Records

IDEP shall maintain proportionate records for significant institutional AI uses.

Routine Tier 1 individual productivity use need not be individually registered.

Tier 2 workflows may require documentation and Tier 3 workflows require proportionate documentation of the purpose, operational review tier, policy use determination, approved system, information processed, required safeguards, responsible owner, human oversight arrangements, and review date.

09. AI Approval and Procurement

AI systems must not be introduced into IDEP operations solely on the basis of convenience, popularity, or individual preference.

Before approving a new AI system or significant use case, IDEP shall consider, as relevant:

- the intended purpose and expected benefit;
- the operational review tier;
- the applicable policy use determination and applicable conditions;
- the applicable legal classification and regulatory requirements;
- data protection and confidentiality;
- information security;
- contractual and data-processing arrangements;
- data retention and use for model training;
- access controls;
- reliability and known limitations;
- human oversight;
- transparency requirements;
- auditability and record-keeping;
- intellectual property considerations;
- accessibility and inclusion;
- fairness, bias, and potential discriminatory effects;
- proportionality and environmental impact.

The depth of assessment shall be proportionate to the nature and risk of the proposed use. Approval shall identify not only the tool but also the purposes and data categories for which it may be used.

Approved AI tools and use cases shall be reviewed periodically and whenever material changes occur that may affect their approval conditions or risk profile.

10. Literacy and Skills Development

IDEP shall take appropriate measures to support the development of AI literacy among personnel and other persons using AI systems on its behalf.

Training and guidance should be proportionate to users' roles, experience, context of use, and the potential impact of the AI systems concerned, and may cover:

- capabilities and limitations of AI;
- verification of AI-generated outputs;
- hallucinations and unreliable sources;
- bias and fairness;
- data protection and confidentiality;
- intellectual property and originality;
- policy use determination and applicable conditions;
- transparency obligations;
- assessment integrity;
- incident reporting.

Personnel involved in higher-risk uses under Section 3 shall receive additional guidance appropriate to their responsibilities.

External evaluators shall receive specific instructions concerning AI use, confidentiality, assessment integrity, and the tools or use cases authorised by IDEP.

11. Incidents and Non-Compliance

Users bound by this Policy must promptly report significant AI-related incidents or concerns through the appropriate IDEP channels.

Relevant incidents may include:

- accidental disclosure of confidential or personal information;
- use of an unapproved AI system for protected information;
- materially inaccurate AI-generated information included in an official output;
- suspected discriminatory or systematically biased outcomes;
- inappropriate reliance on AI in assessment or decision-making;
- failure to comply with legally required transparency measures;
- security incidents associated with an AI system.

IDEP shall respond proportionately to the nature and seriousness of the incident and should consider whether corrective action, additional safeguards, suspension of a use case, training, or policy revision is required.

Non-compliance with this Policy by IDEP personnel may be addressed through applicable internal procedures.

For evaluators, contractors, service providers, or other persons acting on behalf of IDEP, non-compliance may be addressed in accordance with the applicable contract, terms of engagement, instructions, or other governing arrangement.

Annex 1 — Operational Review Matrix

Tier	Typical Uses	Expected Safeguards
Tier 1 — Routine	Grammar and language improvement; formatting; non-sensitive drafting; brainstorming; routine internal correspondence.	Normal human review and validation; standard data protection and security requirements.
Tier 2 — Elevated	Substantive summarisation; preliminary feedback drafting; translation of substantive material; analysis of appropriately prepared programme information; identification of gaps or inconsistencies in materials.	Human validation; accuracy and bias checks; documentation where appropriate; use of an authorised or otherwise suitable AI tool where the information or context requires it.
Tier 3 — Intensive	AI support materially connected with eligibility, scoring, ranking, complaints, funding, rights, or other consequential decisions; processing of protected information requiring enhanced institutional controls.	Enhanced human oversight; appropriate documentation; use of an authorised AI tool or use case where required; data protection, confidentiality, security, or other institutional review where relevant.
Tier 4 — Critical	Delegating final funding, scoring, evaluation, eligibility, or other accountable decisions to AI.	Use must not take place.

This matrix is an operational guide to the tiers and does not constitute or replace the legal classifications established by the EU Artificial Intelligence Act.

Annex 2 — Illustrative AI Use Cases

The following examples illustrate how representative AI uses may be categorised under this Policy. They are not exhaustive. Each example identifies the operational review tier applicable to the use and its policy use determination. A materially different purpose, context, information type, role assigned to AI, or potential impact may constitute a different use and may result in a different tier or determination.

A. Applicants and Beneficiaries

For applicants and beneficiaries, the determinations below are illustrative guidance and should be read in accordance with Section 3. In particular, a Conditional determination indicates that the use is considered appropriate only where any applicable legal, programme, contractual, or organisational prerequisites are satisfied; it does not imply that IDEP's internal authorisation

procedures apply to them. Likewise, a Prohibited determination indicates that the use is considered unacceptable under this Policy; any binding prohibition or consequence arises from applicable legal, programme, contractual, or other requirements rather than from this Policy alone. Applicants and beneficiaries are encouraged to take account of this guidance when using AI in connection with Erasmus+ or ESC activities.

A1 — Language Improvement

Considered Use: An applicant uses an AI tool to improve the grammar and clarity of a proposal.

Operational Review: Tier 1 — Routine

Policy Use Determination: Permitted

Assessment: AI is being used to improve expression rather than substitute for the applicant's project design or judgement. The applicant remains responsible for the final text.

Policy Requirements: The applicant reviews the changes, confirms that the final wording accurately reflects the project, and remains responsible for the final text.

A2 — Project Narrative Drafting

Considered Use: An applicant asks AI to develop a detailed methodology from a short description of the intended project and considers using the generated text in the application.

Operational Review: Tier 2 — Elevated

Policy Use Determination: Permitted

Assessment: The use may be appropriate, but substantial AI-generated text can introduce generic material, assumptions, invented detail, or content that does not accurately reflect the proposed project.

Policy Requirements: The applicant treats the AI response as a draft, checks all factual and programme-related statements, removes unsupported material, and substantially adapts the text so that it accurately reflects the organisation's own plans, capacity, partnership, and project logic.

A3 — Participant Data Analysis

Considered Use: A beneficiary wants to use AI to analyse detailed participant feedback that includes identifiable personal information.

Operational Review: Tier 3 — Intensive

Policy Use Determination: Conditional

Assessment: The analytical objective may be legitimate, but responsible processing depends on the organisation having an appropriate lawful and secure AI environment and satisfying applicable data protection requirements. These conditions cannot be achieved merely through careful prompting.

Conditions for Use: Where identifiable participant information is processed, the organisation must ensure that the processing is lawful and appropriately protected, apply appropriate data minimisation and safeguards, and use an AI environment suitable for the information concerned. If the information is effectively anonymised before analysis, the resulting use constitutes a different use and should be assessed on its own circumstances.

A4 — Project Evidence Fabrication

Considered Use: An applicant asks AI to create plausible statistics, partner experience, references, or evidence that does not exist and includes this material in an application.

Operational Review: Tier 4 — Critical

Policy Use Determination: Prohibited

Assessment: AI must not be used to fabricate or misrepresent information. The applicant remains responsible for the authenticity and accuracy of the application.

B. Reviewers and Evaluators

B1 — Language Assistance

Considered Use: An evaluator uses an AI tool to improve the grammar or clarity of routine administrative text that does not contain application, report, assessment, or other protected information and does not influence the substance of an assessment.

Operational Review: Tier 1 — Routine

Policy Use Determination: Permitted

Assessment: This is a routine supportive use that does not process protected information or affect the evaluator's substantive judgement.

Policy Requirements: The evaluator reviews the changes and remains responsible for the final text.

B2 — Feedback Refinement

Considered Use: An evaluator completes their analysis and early notes or a draft feedback report but asks AI to help turn those notes or draft into formal feedback for the applicant.

Operational Review: Tier 2 — Elevated

Policy Use Determination: Conditional

Assessment: AI may assist with drafting and refinement, but the generated text could alter emphasis, introduce unsupported criticism, or become generic.

Conditions for Use: IDEP must authorise the relevant tool/use for the assessment information concerned. The evaluator provides only information that may lawfully be processed by the authorised tool, checks every substantive point against their own assessment, revises the text as necessary, and accepts responsibility for the final feedback.

B3 — Proposal Summarisation

Considered Use: An evaluator would like an AI system to summarise a lengthy application proposal before completing the assessment.

Operational Review: Tier 3 — Intensive

Policy Use Determination: Conditional

Assessment: Summarisation may be a legitimate support use, but application content is confidential and may contain personal or non-public information. The evaluator cannot independently determine that an external AI service is suitable for processing this material.

Conditions for Use: The activity may take place only if IDEP has approved an AI system specifically for processing the relevant application content and has communicated the applicable conditions to evaluators. The evaluator must still review the source material as required and independently validate the summary. Until IDEP provides such an authorised arrangement, the use must not take place.

B4 — Application Assessment

Considered Use: An evaluator uploads an application to an AI tool, asks it to apply the award criteria, and uses the suggested scores as the basis of the official assessment.

Operational Review: Tier 4 — Critical

Policy Use Determination: Prohibited

Assessment: Substantive scoring and final assessment must remain the evaluator's own expert judgement. AI must not replace or determine an accountable evaluation decision.

C. IDEP Staff and Personnel

C1 — Newsletter Drafting

Considered Use: An IDEP staff member uses an AI tool to prepare a first draft of a newsletter based on public programme information.

Operational Review: Tier 1 — Routine

Policy Use Determination: Permitted

Assessment: This is a routine productivity use provided that the final communication is accurate and subject to appropriate human editorial responsibility. AI assistance does not, by itself, require routine disclosure.

Policy Requirements: The IDEP staff member checks and substantially reviews the text before publication.

C2 — Programme Trend Analysis

Considered Use: IDEP wants to use AI to identify recurring themes across a dataset of project results from which unnecessary identifying information has been removed.

Operational Review: Tier 2 — Elevated

Policy Use Determination: Conditional

Assessment: The use may provide legitimate analytical value, but the output may contain bias, omit nuance, or create misleading generalisations.

Conditions for Use: IDEP must authorise the relevant tool and use case for this institutional analytical workflow. The analytical question should be clearly defined, appropriate data minimisation applied, significant findings verified against the underlying data, and AI-generated patterns treated as analytical support rather than established conclusions.

C3 — Non-Public Data Analysis

Considered Use: A staff member wants to analyse non-public application or grant-management information using AI to identify workload trends, anomalies, or recurring issues.

Operational Review: Tier 3 — Intensive

Policy Use Determination: Conditional

Assessment: The analytical purpose may be legitimate, but the staff member cannot personally authorise an AI system to process non-public institutional information.

Conditions for Use: The analysis may be undertaken only where IDEP has approved the relevant tool and use case, determined which information may be processed, established any necessary data protection and security safeguards, and informed staff of the applicable conditions. Until those institutional conditions are satisfied, the use must not take place.

C4 — Eligibility or Funding Decisions

Considered Use: IDEP uses AI output as the sole or decisive basis for determining whether an applicant is eligible or whether a project should receive funding.

Operational Review: Tier 4 — Critical

Policy Use Determination: Prohibited

Assessment: AI may support appropriately authorised preparatory tasks but must not replace accountable human judgement in final eligibility, assessment, or funding decisions.

Annex 3 — Key Terms and Definitions

Artificial Intelligence (AI): A machine-based system capable of producing outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments. For the purposes of this Policy, the term includes relevant AI functionality embedded in commonly used software.

Generative AI: AI capable of generating new content, including text, images, audio, video, or code, in response to user instructions or other inputs.

AI-assisted output: Content or analysis produced with substantive assistance from an AI system and subsequently used, adapted, or adopted by a human user.

Human oversight: Meaningful human review, judgement, and control over an AI-supported task or process.

Approved AI Tool and Use Case: An AI system and specified purpose that IDEP has authorised under this Policy, subject to any stated limitations concerning data, users, functions, or safeguards.

Unapproved AI Tool: An AI service that has not been authorised by IDEP for the relevant purpose or information, regardless of whether it is freely available, commercially licensed by an individual, or widely used.

Protected Information: Personal, confidential, security-sensitive, commercially sensitive, application-related, or otherwise non-public information requiring protection under law, programme rules, contractual arrangements, or IDEP requirements.

Policy Use Determination: The determination applicable under this Policy to an AI use as Permitted, Conditional, or Prohibited, indicating whether the applicable requirements can be

satisfied directly by the stakeholder, whether an additional prerequisite outside their direct control must be in place, or whether the use must not be undertaken.

Register of Approved AI Tools and Use Cases: The institutional record maintained by IDEP identifying approved AI systems and the purposes, operational review tiers, policy use determination, conditions, information categories, and safeguards associated with their use.

Annex 4 — Reference Framework

This Policy should be read with reference to the following, as applicable. The references are not exhaustive and do not affect the application of other relevant EU or national legislation, programme rules, contractual requirements, or binding European Commission instructions.

EC and Programme Guidance

- European Commission, Guidelines on the Use of Artificial Intelligence in Erasmus+ and European Solidarity Corps Programmes (link)
- European Commission, Guidelines on transparency obligations for providers and deployers of AI systems (link)

Programme Framework

- Erasmus+ Programme Guide 2026 (link)
- European Solidarity Corps Guide 2026 (link)
- European Commission, Erasmus+ Guide for Experts on Quality Assessment 2026 — Actions managed by National Agencies (link)
- European Commission, European Solidarity Corps Guide for Experts on Quality Assessment 2026 (link)

European Union Legislation

- Regulation (EU) 2024/1689 — Artificial Intelligence Act, as amended (link)
- Regulation (EU) 2016/679 — General Data Protection Regulation (link)
- Regulation (EU) 2021/817 establishing Erasmus+: the Union Programme for education and training, youth and sport (link)
- Regulation (EU) 2021/888 establishing the European Solidarity Corps Programme (link)