



Jersey Overseas Aid

Artificial Intelligence (AI) Policy and Procedure

Type (i.e. Policy, Strategy, Procedure, Guideline, protocol)	Policy
Title	AI Policy and Procedure
Version	1.0
Author	Gillian Challinor
Approval Route	Jersey Overseas Aid Commission
Approved by	Edward Lewis
Date approved	August 2026
Review date	August 2027
Linked policies/documents	AI Guidance for Partners

Contents

1. Purpose	3
2. Scope	3
3. Definitions	3
3.1 General Data Protection Terms	3
3.2 AI-Specific Terms	4
4. Legislative and Policy Framework	4
5. Core Principles.....	4
5.1 Lawful and Ethical Use	4
5.2 Human Oversight.....	5
5.3 Fairness and Inclusion.....	5
5.4 Transparency and Explainability.....	5
5.5 Accountability.....	5
5.6 Data Minimisation	5
5.7 Safety and Security	5
5.8 Accuracy and Reliability	5
5.9 Continuous Evaluation	5
6. Permitted Uses of AI	5
7. Restricted and Prohibited Uses	6
8. Selection, Procurement and Vendor Management.....	6
9. Use of General-Purpose AI Tools.....	6
10. Data Protection and Security	7
11. AI Used in Meetings and Recordings	7
12. Risk Management, Deployment and Human Oversight	9
13. Data Subject Rights and AI	9
14. Data Protection Impact Assessments	9
15. Partner Engagement	10
16. Complaints	10
17. Monitoring, Review and Policy Approval.....	10
Appendix A: High-Risk AI Systems under the EU AI Act.....	12
Annex B: Mapping to Government of Jersey AI Policy	13

1. Purpose

This policy sets out how Jersey Overseas Aid (“JOA”) will use artificial intelligence (“AI”) responsibly, ethically, transparently and lawfully in the delivery of its mandate.

JOA recognises the potential of AI to improve efficiency, evidence use and programme delivery. At the same time, JOA is committed to ensuring that AI use does not create harm, exacerbate inequalities, compromise the rights of beneficiaries, donors, partners or staff, or undermine trust in its work.

This policy aims to protect the rights and privacy of data subjects whose data is processed by AI systems including beneficiaries, donors, partners and staff promote transparency and accountability in AI use, and ensure that AI is deployed in a manner consistent with JOA's values and its obligations under the DPJL 2018.

2. Scope

All employees, volunteers, consultants and senior management are responsible for using AI tools in accordance with this policy. They must not enter personal, special category or confidential JOA data into unapproved AI tools, must review AI outputs critically, must be transparent about AI use where appropriate, and must report any concerns to the DPO or their line manager. Annual data protection awareness training includes AI-related content.

This policy applies to:

- All JOA staff (including Programme Associate / intern roles), consultants, Commissioners and advisors;
- All AI systems and AI-enabled features used by, or on behalf of, JOA, whether developed in-house, purchased, licensed or accessed through third-party providers;
- All AI use in programme design, appraisal, monitoring, evaluation and internal operations;
- Procurement and due diligence processes involving AI systems.

Separate guidance is provided for JOA-funded partners.

3. Definitions

For the purposes of this policy, AI refers to digital systems capable of performing tasks that would normally require human intelligence, including generative AI (e.g. text, image or code generation), machine learning and predictive analytics, and automated decision-support tools. The following definitions apply throughout this policy.

3.1 General Data Protection Terms

Personal data: Any data relating to an identified or identifiable, living natural person.

Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic or biometric data processed to uniquely identify a natural person; data concerning health, sex life or sexual orientation; and data relating to a natural person's criminal record or alleged criminal activity.

Processing: Any operation or set of operations performed on personal data, whether or not by automated means.

Controller: The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. JOA acts as the controller for the personal data within the scope of this policy unless otherwise stated.

Processor: A natural or legal person which processes personal data on behalf of a controller.

Data subject: The identified or identifiable living natural person to whom the personal data relates.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory Authority: The Jersey Office of the Information Commissioner (JOIC), the supervisory authority for data protection matters in Jersey.

3.2 AI-Specific Terms

AI system: A machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

Large Language Model (LLM): A category of AI model trained on large volumes of text and capable of generating, summarising or transforming text in response to natural-language prompts. Common public LLM-based tools include ChatGPT, Microsoft Copilot, Google Gemini, Anthropic Claude and Perplexity.

High-risk AI system: An AI system classified as high-risk under Article 6 and Annex III of the EU AI Act. The list of high-risk uses is reproduced at Appendix A of this policy for reference.

General-Purpose AI tool: A consumer or business AI tool, typically built on an LLM, used for general tasks such as drafting, summarising, research or analysis. JOA draws a distinction between general-purpose tools of this kind and AI systems that are purpose-built into JOA's business systems.

Profiling: Any automated processing of personal data intended to evaluate, analyse or predict aspects of a data subject's personal characteristics, behaviour, performance, economic situation, health, preferences, interests, reliability, location or movements.

4. Legislative and Policy Framework

JOA's use of AI is governed by the following legislation and internal policies:

- The Data Protection (Jersey) Law 2018 (the "DPJL 2018");
- Guidance and strategic priorities published by the Jersey Office of the Information Commissioner (JOIC);
- The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) used as a good-practice reference framework, particularly for risk classification and human oversight, where Jersey law does not itself legislate on AI;
- JOA's Data Protection Framework Policy;
- JOA's Data Protection Impact Assessment Policy and Procedure;
- JOA's Data Rights Policy and Procedure;
- JOA's Data Breach Notification Policy and Procedure;
- JOA's AI Guidance for Partners.

5. Core Principles

JOA will ensure that all use of AI aligns with the following principles, which reflect both JOA's own values and the requirements of the DPJL 2018, using the EU AI Act as a reference point of good practice:

5.1 Lawful and Ethical Use

AI must comply with relevant laws, including data protection and safeguarding requirements, and align with international development ethics. AI systems must be used in a manner that respects human dignity, rights and freedoms, and must avoid bias, discrimination or harm. JOA will not engage in any AI practice that is prohibited.

5.2 Human Oversight

AI will support, not replace, human judgement. Final responsibility for decisions remains with the JOA Commission and staff. Significant decisions affecting individuals will not be made by AI systems without meaningful human oversight.

5.3 Fairness and Inclusion

JOA will take reasonable steps to identify and mitigate bias in AI systems and ensure that their use does not disadvantage individuals, communities or countries.

5.4 Transparency and Explainability

JOA will be transparent about where AI is used to facilitate decision-making processes, in line with Article 12 of the DPJL 2018, and will ensure any documentation and outputs can be explained where necessary.

5.5 Accountability

Clear accountability will be maintained for all decisions supported by AI tools. JOA accepts accountability for the AI systems it uses, including those provided by third parties.

5.6 Data Minimisation

JOA will use only the data necessary for the intended AI use case, and will not provide personal, special category or confidential data to AI tools beyond what is necessary for that purpose.

5.7 Safety and Security

AI systems must be used in a way that protects sensitive information and minimises risks to individuals and organisations. The AI systems will not train on the organisations inputs or outputs, the organisation owns its data, and the processing is under contractual confidentiality.

5.8 Accuracy and Reliability

JOA will take reasonable steps to ensure that AI-generated outputs are accurate and appropriate for their intended use. AI outputs are verified against reliable sources, particularly where they inform programme, funding or strategic decisions.

5.9 Continuous Evaluation

AI systems will be subject to ongoing monitoring and evaluation to ensure they continue to function as intended and remain compliant with this policy and applicable law.

6. Permitted Uses of AI

Subject to the requirements of this policy, JOA may use AI in the following ways:

- Programme design, appraisal, monitoring and evaluation support, subject to human review of any output that informs a funding or strategic decision
- Beneficiary or partner service automation, including chatbots and virtual assistants, where the user is clearly informed that they are interacting with an AI system.
- Drafting, summarising, translating and proof-reading documents and communications, subject to human review;
- Research, analysis and benchmarking;
- Cybersecurity threat detection and response;

- Administrative automation such as scheduling, data entry, transcription and reporting.

All AI output is treated as a draft and is verified by the responsible user who retains full professional responsibility.

No decisions relating to programme funding or other strategic matters that have similarly significant effects on a data subject are made solely through automated processing. All such decisions are subject to meaningful human review and are made by the appropriate responsible member of staff at JOA.

7. Restricted and Prohibited Uses

Without explicit approval, AI must not be used for:

- Making final funding or investment decisions;
- Processing sensitive or personal data in unsecured systems;
- Safeguarding case management;
- Any use that could compromise the confidentiality of partners or beneficiaries;
- Automated profiling or scoring of applicants, partners or beneficiaries without appropriate human oversight and review;
- Recruitment, selection or other employment-related decision-making without appropriate human oversight, transparency and review.

JOA will not engage in any prohibited AI practices.

8. Selection, Procurement and Vendor Management

Before JOA adopts a new AI system or AI-enabled feature, the proposal must be reviewed by the DPO and, where applicable, by the IT lead and senior management. The assessment includes:

- The purpose of the AI system and the problem it is intended to solve;
- Whether the AI system processes personal data, and if so, the categories of data and data subjects involved;
- Whether the AI system falls into any high-risk category.
- The vendor's compliance with data protection laws, the location of data processing, and any cross-border transfer implications;
- Whether a DPIA is required under the DPJL 2018
- The technical and organisational security measures applied to the AI system;
- Evidence of bias mitigation and transparency of system design;
- Environmental and social impacts, including consideration of the energy use and carbon footprint of AI systems where this is material and proportionate.

Where the AI system involves processing of personal data by a third party, the engagement is governed by a Processor Agreement meeting the requirements of Article 19 of the DPJL 2018. Where the AI system processes personal data outside Jersey, JOA's Data Transfer Policy and Procedure applies.

9. Use of General-Purpose AI Tools

General-purpose AI tools such as ChatGPT, Microsoft Copilot, Google Gemini, Anthropic Claude and similar services are widely available. JOA permits the use of such tools for legitimate work purposes, subject to the following requirements:

- Personal data, special category data, beneficiary information, donor information, partner information, financial information, employment information or other confidential JOA data must not be entered into a general-purpose AI tool unless the specific tool, account configuration and use case have been approved in advance by the DPO and the IT lead;
- Where approved, use must be through JOA's licensed or enterprise version of the tool, configured to disable training on inputs and to provide appropriate data residency, rather than through personal or free-tier accounts;
- Outputs of general-purpose AI tools must be reviewed by a human before being used, published or acted upon. AI outputs may contain errors, fabrications ("hallucinations") or biased material, and the user remains responsible for the accuracy and appropriateness of the work product;
- Users must be transparent about material use of AI in work outputs where transparency is required by professional standards, contracts, regulators, or the EU AI Act (Article 50), for example where content is synthetic media;
- Users must not use AI tools in a manner that breaches third-party intellectual property rights, professional regulatory requirements or JOA's code of conduct.

10. Data Protection and Security

JOA staff must:

- Avoid entering confidential, personal or sensitive data into publicly available AI tools;
- Use approved systems where sensitive data is involved;
- Comply with Government of Jersey data protection requirements and the DPJL 2018.

In line with the data minimisation principle, JOA uses only the data necessary for the intended AI use case. Where personal data is processed by an AI system, data subjects are informed through JOA's Privacy Notice.

All AI-related processing activities are documented in JOA's Record of Processing Activities (ROPA), maintained under Article 14 of the DPJL 2018. The use of AI features within existing systems (for example, AI-enabled features within productivity, grant management, fundraising, beneficiary management or HR platforms) is also recorded, so that JOA maintains an accurate inventory of where AI is deployed.

11. AI Used in Meetings and Recordings

Where AI tools are used to record, transcribe or summarise meetings (whether through a meeting platform's built-in feature or an external AI assistant), the use must comply with the following requirements:

- All participants must be informed that the meeting is being recorded or transcribed, the purpose of the recording, who will have access to it, and how long it will be retained. Where consent is the lawful basis, that consent must be obtained from all participants at the start of the meeting;
- Recordings and transcripts must be stored securely and accessed only by authorised personnel;
- Retention is limited to what is necessary for the stated purpose. Where the purpose is the production of minutes, audio recordings should be deleted once a written transcript or set of minutes has been verified;
- The DPO must approve any extended retention of recordings.
- Where visual recording is available as a feature, it is disabled by default unless a specific case has been made and approved by the DPO.

Specific retention periods are set out in JOA's Data Retention Schedule.

12. Risk Management, Deployment and Human Oversight

JOA will apply a proportionate, risk-based approach to AI use. AI use will be assessed as:

- Low risk: routine administrative or drafting support;
- Medium risk: analytical or summarisation tasks that inform decisions;
- High risk: use cases that involve sensitive data, vulnerable populations, beneficiaries, or that influence funding or strategic decisions, or that fall within a high-risk category.

High-risk uses require documented justification, appropriate approval, and additional review and oversight.

Before an AI system is deployed, it must be tested and validated to confirm that it functions as intended without causing demonstrable harm or bias. Staff involved in using or interpreting the AI system's outputs receive training on its appropriate use, its limitations, and the procedure for raising concerns.

Consistent with the EU AI Act's approach to human oversight, AI systems that affect individuals (including profiling, automated decision-making and AI-driven analytics) operate under meaningful human oversight. An identified individual within JOA is responsible for the operation of each significant AI system; that individual must be able to intervene, override or disregard the AI system's output.

AI systems are reviewed at least annually to confirm that they continue to comply with this policy, the DPJL 2018 and (where relevant) the EU AI Act. Internal reviews assess effectiveness, data protection compliance, ethical use and stakeholder impact. The DPO reports findings to the JOA Commission.

13. Data Subject Rights and AI

Data subjects retain all of the rights set out in JOA's Data Rights Policy and Procedure when their personal data is processed by an AI system. Two rights are of particular relevance in the AI context:

Right regarding automated individual decision-making (Article 38, DPJL 2018) — Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, subject to specified exceptions. Where JOA relies on an exception, it ensures the data subject's rights and legitimate interests are safeguarded, including by providing meaningful human intervention, an opportunity to express the data subject's point of view, and the right to contest the decision.

Right to explanation (EU AI Act, Article 86) — Where a decision is taken by a deployer of a high-risk AI system on the basis of the system's output, and that decision produces legal effects or similarly significantly affects the data subject, the data subject has the right to obtain a clear and meaningful explanation of the AI system's role in the decision-making process and the main elements of the decision taken. JOA applies this as good practice even in cases falling outside the direct scope of the EU AI Act.

Requests to exercise these rights are handled by the DPO in accordance with JOA's Data Rights Policy and Procedure, and are recorded in the Data Rights Log.

14. Data Protection Impact Assessments

Before JOA deploys an AI system, the DPO determines whether a Data Protection Impact Assessment (DPIA) is required under Article 16 of the DPJL 2018. A DPIA will be required in particular where the AI system involves:

- Systematic and extensive automated evaluation of personal aspects (including profiling), on which decisions are based that produce legal or similarly significant effects;
- Processing on a large scale of special category data;

- Systematic monitoring of a publicly accessible area on a large scale;
- Processing of personal data relating to children or vulnerable adults, including vulnerable beneficiaries of JOA-funded programmes;
- Use of new or innovative technologies that may impact privacy;
- Matching or combining datasets in ways the data subject would not reasonably expect.

Where the AI system falls into a category classified as high-risk under Article 6 and Annex III of the EU AI Act (see Appendix B), JOA treats this as a strong indicator that a DPIA is required and will normally complete one. Detailed procedures for completing DPIAs are set out in JOA's Data Protection Impact Assessment Policy and Procedure.

15. Partner Engagement

JOA will provide guidance to partners on responsible AI use. Partners are expected to:

- Maintain human oversight;
- Protect data and confidentiality;
- Use AI transparently and responsibly.

Further detail is set out in JOA's AI Guidance for Partners.

The JOA Commission maintains strategic oversight of JOA's use of AI, approves this policy, and receives regular reports from the DPO on AI deployments, risks and incidents.

Data Protection Officer

The DPO has operational responsibility for ensuring that JOA's use of AI complies with the DPJL 2018 and (where relevant) the EU AI Act. This includes advising on AI selection and procurement, determining whether a DPIA is required, reviewing DPIAs for AI systems, maintaining the AI inventory, providing guidance to staff, monitoring developments in AI law and regulation, and reporting to the JOA Commission. The DPO is not personally responsible for JOA's data protection compliance; as controller, JOA remains accountable.

16. Complaints

If a data subject is dissatisfied with how JOA has dealt with an AI-related matter, they should be advised to invoke JOA's complaints process by writing to the DPO:

Data Protection Officer Jersey Overseas Aid 2nd Floor, 24 Sand Street, St Helier, Jersey Email: dataprotection@joa.je

Data subjects also have the right to lodge a complaint with **the Jersey Office of the Information Commissioner**, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT; telephone +44 (0)1534 716530; email enquiries@jerseyoic.org website www.jerseyoic.org.

17. Monitoring, Review and Policy Approval

JOA will:

- Review this policy annually, or sooner where there are significant changes to legislation, JOIC guidance, the EU AI Act, AI technology, or JOA's operational practices;
- Update guidance in line with emerging risks and opportunities;
- Assign responsibility for oversight of AI use within the organisation;

- Ensure staff receive appropriate training on responsible AI use and undertake any mandatory Government of Jersey training;
- Promote continuous learning and responsible innovation as AI technologies evolve.

Any incidents involving AI use (e.g. data breaches, misuse or harmful outputs) must be reported and managed in line with JOA's existing data protection and safeguarding procedures.

Appendix A: High-Risk AI Systems under the EU AI Act

Under Article 6 of the EU AI Act, an AI system is classified as high-risk if it falls into one of the categories set out in Annex III of the EU AI Act (extracted below). This appendix is for reference only; before relying on it, the current text of Annex III should be checked at the EU AI Act online repository, as Annex III may be amended.

Annex III categories include:

- Biometrics (where their use is permitted under relevant law): remote biometric identification systems; biometric categorisation systems according to sensitive or protected attributes or characteristics; and emotion recognition systems. Biometric verification systems intended solely to confirm that a specific natural person is the person they claim to be are excluded.
- Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.
- Education and vocational training: AI systems used to determine access or admission, to assign individuals to institutions, to evaluate learning outcomes, to assess appropriate levels of education, or to monitor and detect prohibited behaviour during tests.
- Employment, worker management and access to self-employment: AI systems used for recruitment, screening, evaluation, promotion, termination, task allocation and performance monitoring.
- Access to and enjoyment of essential private services and essential public services and benefits: AI systems used for eligibility determination, creditworthiness scoring, risk assessment and pricing in life and health insurance, and emergency dispatching.
- Law enforcement: certain AI systems used for risk assessment, polygraphs, evidence evaluation and crime analytics.
- Migration, asylum and border control management.
- Administration of justice and democratic processes: AI systems used by judicial authorities or to influence elections or referenda.

Where Jersey Overseas Aid is considering deploying an AI system that may fall into any of these categories, the DPO must be consulted, a DPIA will normally be required, and the EU AI Act's high-risk requirements (Articles 8 to 15) should be considered as a reference framework even where the system is not directly subject to the EU AI Act.

Annex B: Mapping to Government of Jersey AI Policy

The table below maps JOA's policy to the core principles typically set out in the Government of Jersey AI Policy.

Government of Jersey Principle	JOA Policy Reference	How It Is Reflected
Lawfulness	Sections 4.1, 8	Explicit requirement to comply with data protection, safeguarding, and legal obligations
Ethical Use	Sections 1, 4.1	Commitment to avoiding harm, protecting rights, and aligning with development ethics
Human Oversight	Sections 4.2, 5, 6	AI cannot replace human judgement; all outputs must be reviewed
Transparency	Section 4.4	Requirement to document and explain AI use where relevant
Accountability	Section 4.5	Clear responsibility remains with JOA staff, not AI systems
Fairness / Bias Mitigation	Section 4.3, 9	Active consideration of bias in tools and procurement
Safety and Security	Sections 4.6, 8	Strong emphasis on data protection and safe use
Proportionality / Risk-Based Approach	Section 7	Higher-risk uses subject to additional safeguards
Governance and Oversight	Sections 2, 11	Defined scope, review mechanism, and organisational responsibility
Responsible Innovation	Sections 1, 11	Balanced approach enabling AI use while managing risk