Australian Library and Information Association

Artificial Intelligence Procedures

August 2026



Contents

1. Purpose 3
2. Artificial Intelligence Definition 3
3. Scope 3
4. Approved Uses of AI 4
5. Risk Assessment 4
6. Use of Private / In-house AI Systems 4
   6.1. General 4
   6.2. Assessment process 5
7. Use of Public AI Systems 5
7.1. General 5
   7.2. Low-risk uses 5
   7.3. Higher-risk uses 6
8. Privacy and Data Protection 6
9. Copyright and Intellectual Property 6
   9.1. Inputs 6
   9.2. Outputs 7
10. Indigenous Cultural and Intellectual Property 7
11. Output checking 7
12. Transparency and Disclosure 7
13. Environmental Sustainability 8
14. Misinformation and Deepfakes 8
15. AI Incident Reporting 8
16. Training and Awareness 9

Attachment: Risk Matrix (Optional) 10

Attachment: AI Rules of Thumb 11

This procedure is written to supplement the ALIA Artificial Intelligence Policy and should be read in context with it. Certain elements, such as the Definition of AI and scope, are duplicated in the AI Policy.

Purpose

This procedure sets out guidelines for use of artificial intelligence (AI) technologies by the Australian Library and Information Association (ALIA).

It has been written to supplement the ALIA Artificial Intelligence Policy (AI Policy) and is intended to assist staff and other ALIA representatives to implement the principles in the Policy.

As with the AI Policy, it is intended to:

- Support the responsible use of AI to enhance services to members and advance ALIA's strategic objectives; and
- Provide a clear framework for identifying, assessing and managing risks associated with AI systems

1. Artificial Intelligence Definition

For the purpose of this procedure, AI is defined as any technology that uses data to make inferences and generate outputs such as predictions, recommendations or decisions with a degree of autonomy. This includes but is not limited to:

- Machine learning models
- Generative AI tools
- Predictive analytics systems
- Chatbots that generate their own responses

2. Scope

This procedure covers:

- Publicly available AI tools (e.g. ChatGPT, Claude, Gemini, image generation tools)
- Enterprise AI tools embedded in licensed software (e.g. Microsoft Copilot)

- Any future private, bespoke or in-house AI systems developed, procured or promoted by ALIA

It does not replace existing policies on privacy, security, records management, copyright, or acceptable ICT use, but should be read alongside them.

3. Approved Uses of AI

AI may be used to support ALIA's work, as long as the use is lawful, ethical and aligned with the ALIA AI Policy.

AI must not be used as the sole or primary basis for decisions that materially affect individuals, organisations or the determination of ALIA policy positions.

Factors such as reputational risk or environmental impact should be considered when deciding whether to use AI for a particular task.

4. Risk Assessment

Before using AI, ALIA representatives must assess whether the proposed use is low, medium or high risk, taking into account the nature of the use, the likely impact of the use, and the AI tool/s being used.

This assessment determines what if any risk management measures are needed as part of the use.

When assessing the risk of an AI use you should consider:

- Type of data used – eg public vs personal/confidential
- Purpose of the use - eg whether it involves decision making
- Potential impact on individuals or organisations
- Likelihood and consequence of error
- Legal or regulatory implications
- Reputational impact on ALIA

A risk matrix is provided as Attachment A to assist with assessments.

5. Use of Private / In-house AI Systems

5.1. General

ALIA may approve the use of private or in-house AI systems, which are intended to be used internally and do not share data or inputs with external companies such as the software provider.

Licensed enterprise tools (eg Microsoft Copilot, IMIS) are not considered private/in-house AI unless they have been assessed and approved as such via the process below. Staff should be aware that data input to these tools may be accessed and used by the vendor and should treat them as public AI tools.

5.2. Assessment process

Before any private or in-house AI system is adopted a written proposal must be prepared including:

- A project plan describing:
  - The technology
  - Intended use cases
  - Proposed data inputs and outputs
  - Risks and mitigations
- A risk assessment confirming the system is safe, secure and dependable

The proposal must be approved by the Chief Executive Officer for low or medium risk uses or the Board where the use is assessed as high risk. Board approval is required if ALIA seeks to develop or commercialise an AI product.

Once deployed:

- Systems must be monitored for performance, bias, accuracy and emerging risks
- Regular reviews must be undertaken

6. Use of Public AI Systems

6.1. General

Public AI tools are tools that are made openly available to the public on general terms and that are not part of an enterprise agreement specific to ALIA e.g. Claude, ChatGPT, or the standard implementation of Co-Pilot.

6.2. Low-risk uses

Staff may use public AI tools for uses that have been assessed as low-risk, provided normal precautions set out below are followed.

Examples of low risk uses include:

- Summarising publicly available documents
- Drafting or editing publications or communications
- Brainstorming ideas
- Research support

- Creating non-sensitive images or graphics

6.3. Higher-risk uses

Public AI tools should not generally be used for medium or high risk uses that may impact the organisation, staff, members or stakeholders.

In specific cases public AI tools may be used for medium or high risk uses, as long as approval is first obtained from a Manager (medium risk) or CEO (high risk) through a documented risk assessment.

Examples of higher-risk uses include:

- Using AI to support decision-making processes
- Using AI with any non-public, confidential or personal information
- Using AI with any material that contains Indigenous Cultural and Intellectual Property (ICIP)
- Generating content presented as official ALIA advice or policy

7. Privacy and Data Protection

- Personal information of staff or members must not be entered into public AI tools, and may only be used with inhouse-systems if the use of the data has been assessed and approved per clause 7.3.
- Data sharing should be disabled on any AI system where possible. This may sometimes be listed as model training.
- Any AI system handling personal data must comply with ALIA's privacy obligations.
- Data minimisation principles should be applied: only use what is necessary.

8. Copyright and Intellectual Property

8.1. Inputs

Third party copyright materials must not be copied or uploaded as inputs to AI unless:

- permission is obtained from the rights-holder
- they are licensed to allow reuse (eg Creative Commons Attribution licensed material) or
- the use is covered by an exception in the Copyright Act 1968.

Links to material that is freely available online maybe provided to an AI for its reference.

ALIA's own materials may be uploaded to AI systems as long as they are publicly available or appropriate to be made publicly available, and do not include personal, confidential or sensitive information.

If in doubt, seek advice from your manager before using copyright material as an AI input.

8.2. Outputs

- When using generative AI tools, staff must endeavour to ensure:
    - AI-generated material does not reproduce protected content
    - Proper attribution to source materials is provided where possible eg through a transparency notice per below
- AI outputs will only be protected by copyright if sufficient human input has been involved. However, this can be difficult to determine on a case-by-case basis. If in doubt, assume any AI outputs you encounter are protected by copyright.
- If in doubt, seek advice from you manager before publishing or distributing AI-generated content.

9. Indigenous Cultural and Intellectual Property

Material that contains Indigenous Cultural and Intellectual Property (ICIP) may not be copied or uploaded as an input to AI unless:

- prior and informed consent is obtained from the relevant community
- appropriate protocols relating to the use of the material have been followed.

10. Output checking

Before being published or used to support decisions, all AI outputs must be reviewed by a human to check:

- Accuracy
- Bias or harmful content
- Copyright or intellectual property concerns

11. Transparency and Disclosure

ALIA will disclose significant uses of AI in:

- Public-facing content
- Research outputs
- Decision making processes

- Policy development processes

This disclosure can be made in any reasonable manner, but by preference should be included in a written transparency notice which is published on appropriate communications channels either:

- before the use, where it is anticipated that AI will be used eg if AI is to be used to assist with a recruitment process
- upon publication of outputs from AI use.

12. Environmental Sustainability

ALIA recognises that AI systems consume significant computational and energy resources and therefore have environmental impacts.

Staff are expected to:

- Use AI only where it provides a clear work-related benefit
- Avoid using AI for personal or recreational purposes on ALIA systems or accounts
- Prefer simpler or lower-resource options where they can reasonably achieve the same outcome
- Avoid unnecessary repeated prompting or generation

When choosing whether to use AI, staff should consider whether the task can be completed as effectively without AI, or with existing non-AI tools.

Responsible, proportionate use of AI supports ALIA's broader commitment to sustainability.

13. Misinformation and Deepfakes

Staff should remain alert to the risk of misinformation, manipulated content and AI-generated deepfakes when using online resources or AI tools.

Where information is important, sensitive, or likely to be relied upon:

- Verify against trusted, authoritative sources
- Use multiple independent sources where possible
- Treat sensational, emotionally charged or unusually definitive content with caution

14. AI Incident Reporting

Staff must promptly report any suspected or actual AI-related incident, including:

- Accidental or unauthorised disclosure of personal, confidential or sensitive information
- Use of AI in a way that breaches this policy
- Significant inaccuracies or harmful outputs that could cause material impact to the organization, staff, members or stakeholders
- Security vulnerabilities or suspected compromise involving AI tools

Reports should be made as soon as practicable to the staff member's manager and the Director of Policy, Education, Research and Training or Chief Operating Officer/IT Manager.

ALIA will:

- Assess and record reported incidents
- Take appropriate remedial action
- Notify affected parties or regulators where required
- Continue to educate and support staff, members and the public on risks associated with AI, such as deepfakes and misinformation

15. Training and Awareness

ALIA will support staff by:

- Providing guidance on responsible AI use
- Sharing updates on risks and good practice

Staff are encouraged to stay informed about emerging AI issues.

Attachment: Risk Matrix (Optional)

Risk Level	Data Used	Tool used	Impact	Typical Examples	Approval Required
Low	Public, non-sensitive information	Proprietary closed system, that has been assessed and approved for use	Does not materially impact organisational decisions or member outcomes	Drafting emails, summarising public reports, brainstorming ideas	None (staff discretion)
Medium	Internal but non-sensitive information	Public system which has been assessed and approved for use, and for which data controls are enabled; or internal closed system	May influence a non-critical organisational decision or member outcome	Drafting documents, analysing internal trends	Manager approval
High	Personal, confidential, sensitive or indigenous information	Public system which has not been assessed and for which data controls are not enabled	Influences critical organisational decisions or member outcome	Member data analysis, policy recommendations, automated decision making	Executive approval

If unsure, staff should treat the use as higher risk and seek advice.

Attachment: AI Rules of Thumb

When using AI tools:

- Always assess whether your use is low, medium or high risk and take precautions appropriate to the risk level
- Disable data sharing and model training options where possible
- Unless appropriate permissions have been obtained, never upload or link to:
    - Confidential or sensitive information that has not been made publicly available and is not appropriate to be made publicly available
    - Personal or private staff or member information
    - Third-party copyright material not openly available online
    - Indigenous Cultural and Intellectual Property

  Any use involving such material must be treated as high risk and cleared at an appropriate level (see Procedures).
- Review all materials created by AI tools and assess them for accuracy, bias, harmful content or copyright infringement before they are used or publicly release.
- Consider potential harms to ALIA, its staff, members or other stakeholders when deciding whether to use an AI, including reputational or environmental harms.
- If in doubt, discuss your proposed use with your manager.