



Artificial Intelligence (AI) Use Policy

July 2026

1. Purpose and Scope

1.1 This policy outlines the acceptable use of Artificial Intelligence (AI) tools, including Microsoft Copilot and similar systems, at Ashgrove West Preschool Centre Inc. (“AWPS” or “the Centre”). It applies to all staff, volunteers, and other personnel who may access or use AI tools in connection with the Centre’s operations.

1.2 This policy supports the safe, ethical, transparent, and lawful use of AI in a way that protects children, families, staff, and the broader AWPS community.

1.3 This policy is informed by and operates in alignment with relevant privacy obligations, child safety expectations, and educational guidance.

1.4 This policy also supports AWPS to manage the use of AI tools in a way that maintains professional standards, protects confidential information, and supports the effective operation of the Centre.

2. Guiding Principles

AWPS is committed to the use of AI tools in a manner that is:

- Child safe and privacy protecting
- Ethical and professional
- Transparent and accountable
- Supportive of professional judgement rather than a substitute for it
- Aligned with applicable law, regulation, and sector guidance

3. Definitions

For the purposes of this Policy:

3.1 Artificial Intelligence (AI): Digital systems that generate, summarise, analyse, or transform content in response to user prompts or instructions.

3.2 Approved AI tools: AI products or features approved by AWPS for work-related use, including organisation-managed Microsoft Copilot tools where applicable.

3.3 Personal information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.

3.4 Sensitive information: Personal information requiring a higher level of protection, including health information, behavioural information, child protection information, cultural or religious information, Aboriginal and Torres Strait Islander status, and other confidential records relating to children, families, or staff.

4. Approved Uses of AI

4.1 Staff may use approved AI tools for work-related tasks that do not involve the entry or disclosure of personal, sensitive, or identifying information.

4.2 Examples of permitted use include drafting general communications, generating activity or lesson ideas, preparing policy or administrative documents, developing templates, and supporting professional learning.

4.3 AI may be used to support productivity within approved Microsoft 365 applications where the data is already securely stored within the organisation's environment and existing access controls remain in place.

5. Prohibited Uses of AI

5.1 Staff must not enter, upload, paste, or otherwise disclose names, photos, medical information, behavioural records, enrolment records, contact details, or any other identifying information about children, families, or staff into AI chat tools unless expressly approved and lawfully permitted.

5.2 AI tools must not be used to prepare incident reports, behaviour reports, child assessments, or to make decisions, recommendations, or professional judgements regarding a child's development, behaviour, safety, wellbeing, or educational program.

5.3 Staff must not use personal AI accounts or unapproved third-party AI services for work-related tasks involving AWPS information.

5.4 AI tools must not be used to generate, analyse, or interpret images of children, or to produce content that may compromise child safety, dignity, privacy, or confidentiality.

6. Data Privacy and Security

6.1 Any use of AI tools must comply with applicable privacy and confidentiality obligations, including the protection of personal and sensitive information held by the Centre.

6.2 Where Microsoft Copilot or similar tools are used within approved organisational systems, staff must ensure that use remains within the Centre's secure environment and is consistent with access controls, retention requirements, and any applicable organisational settings.

6.3 Where a significant data breach involving children's or families' personal or sensitive information occurs through the use of an AI tool, the Director must promptly notify the Management Committee and manage the incident in accordance with the Centre's Privacy and Data Breach procedures.

6.4 Staff must ensure that any AI-generated content used by the Centre does not infringe copyright, intellectual property rights, or licensing requirements and must verify the appropriateness of any material before publication or distribution.

7. Staff Responsibilities

7.1 All staff must use AI tools ethically and professionally, in accordance with this Policy.

7.2 Staff are responsible for applying professional judgement and verifying the accuracy and appropriateness of AI-generated content before use.

7.3 Staff must ensure their use of AI tools is safe, responsible, and consistent with organisational expectations

7.4 AI-generated content must be reviewed and approved by the relevant staff member before it is relied upon, distributed, published, or incorporated into Centre records.

8. Leadership Responsibilities

8.1 Leadership is responsible for determining which AI tools are approved for workplace use and for communicating any limitations, controls, or requirements associated with those tools.

8.2 Leadership must ensure staff are supported in using AI tools appropriately, oversee compliance with this Policy, and act on any misuse or identified risks

9. Consequences of Misuse

9.1 Misuse of AI tools, or any use inconsistent with this Policy, may result in corrective action including retraining, removal of access to AI tools, disciplinary action, or reporting to relevant authorities where required.

10. Policy Review

10.1 This Policy will be reviewed annually, or earlier if significant changes occur in technology, legislation, regulatory guidance, or organisational requirements.

10.2 Any proposed amendments to this Policy must be reviewed and approved by the Management Committee before they are implemented.

10.3 Any updates to this Policy will be communicated to staff and other relevant members of the AWPS community as appropriate.

Approved By Management Committee

Date Adopted __21__ / __07__ / __2026__

Next Review Due __06__ / __07__ / __2027__