THE HUTCHINS SCHOOL

Generative AI usage policy

Relevant legislation	Anti-Discrimination Act 1998 (Tas) Australian Curriculum, Assessment and Reporting Authority (ACARA) Australian Cyber Security Centre (ACSC) Guidelines Australian Privacy Principles (APPs) Child Safe Standards Framework (Tas) Disability Discrimination Act 1992 (Cth) Education Act 2016 (Tas) Notifiable Data Breaches (NDB) Scheme Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) Tasmanian Assessment, Standards and Certification (TASC) Privacy Act 1988 (Cth)
Commencement date	01 March 2025
Last review date	01 March 2025

1. Purpose

The purpose of this policy is to outline The Hutchins School's standards for safe, responsible and ethical use of Generative Artificial Intelligence (Generative AI) tools. It has been produced to align with the Australian Framework for Generative AI in Schools and to reflect the requirements of The Privacy Act 1988 (Cth).

2. Scope

This policy applies to Hutchins staff and students using Generative AI tools for communication, teaching and learning activities, administration or other school-related activities. It does not cover the use of Predictive Artificial Intelligence.

3. Definitions

Generative Artifical Intelligence	Generative AI can generate new content such as text, images, audio and video that resembles what humans can produce. It is effective at recognising patterns (in video, audio, text or images) and emulating them when tasked with producing something. *Source: Australian Framework for Generative Artificial Intelligence in Schools*
Intellectual Property (IP)	This policy distinguishes between two definitions in order to provide clarity to what may and may not be shared with Generative AI. These definitions are: **Intellectual Property**, which includes but is not limited to:

	• curricula; • teaching materials; • policies; and • branding. Generally speaking, Intellectual Property that is already publicly accessible or available online in very similar forms (e.g. a blank Individual Learning Plan template) may form part of a Generative AI prompt without concern (if it is blank and does not contain personal or sensitive information, as defined here). **Protected Intellectual Property (IP)**, which includes (but is not limited to): • school-owned or generated research; • training modules or presentations created for internal use; • proprietary systems developed by the School; • resources purchased for or generated by the School for internal use; • strategic planning documentation; and • any documentation explicitly marked as ‘confidential’. Protected IP remains the exclusive property of the School, and must not be shared, reproduced or distributed, including with Generative AI.
Personal Information	“Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.” *Source: The Privacy Act 1988 (Cth)*
Predictive Artificial Intelligence	Predictive artificial intelligence (AI) involves using statistical analysis and machine learning (ML) to identify patterns, anticipate behaviors and forecast upcoming events. *Source: IBM corporation*
Sensitive Information	“Information… about an individual” such as: • racial or ethnic origin; • political opinions; • membership of a political association; • religious beliefs or affiliations; • philosophical beliefs; • membership of a trade union or professional association; • sexual orientation or practices; • criminal record; • health information; • genetic information; and • biometric information used for automated biometric verification or identification.

	Source: The Privacy Act 1988 (Cth)
Prompt	Information supplied by a person to a Generative AI with the purpose of generating a response. A prompt may be a question, piece of text, code, image or example.

4. Key accountabilites

This policy is designed to support staff and students in the use of Generative AI (also: GenAI) tools in ways that enhance learning and wellbeing. Generative AI tools can be valuable in supporting educational outcomes for learners and reducing workloads for staff, but it is important that their use is fair, ethical and within the boundaries and guidelines established by the School, by legislation and by best practice organisations.

Generative AI tools may be used by staff and students at the School:

- to support and enhance teaching and learning;
- for the benefit of all members of the school community; and
- in ways that are inclusive, accessible, fair and respectful.

Managers and supervisors are responsible for:

- supporting Generative AI practices that protect the privacy, security and safety of all members of the school community;
- adhering to copyright obligations and complying with relevant legislation;
- engaging staff in learning about Generative AI tools and their benefits, risks, limitations and biases;
- supporting staff and students in the use of Generative AI in ways that are ethical and safe, preserving human agency, accountability, and decision-making;
- supporting staff compliance with Standard 7 of the Standards for the Provision of TASC-accredited Senior Secondary Courses;
- providing guidance in the use of School-approved Generative AI tools and informing staff and students with respect to tools that may compromise security; and
- ensuring that students and families have access to clear and appropriate information and guidance on the use of Generative AI in line with Academic Integrity Protocols (see supporting/related documents).

Staff are responsible for:

- ensuring safe, ethical and compliant use of Generative AI within the scope of their work and role;
- using Generative AI tools in line with existing curriculum, procedures, standards and guidelines (see supporting/related documents);
- ensuring that prompts used to produce Generative AI outputs do not include:
  - **‘Personal Information’** regarding staff, students or members of the School community;

  - **‘Sensitive Information’** that can be linked to specific individuals (either through the inclusion of personal information or through context);
  - **Confidential or identifiable school data** (e.g. performance reviews, financial data, assessment or exam details, strategic or operational documents) that can be linked back to individuals or the School (either through the inclusion of personal information or through context); or
  - **Protected Intellectual Property (IP)** (as defined above);

If staff are unsure whether certain types of data may be shared with Generative AI they must contact the IT team for support and advice.

- understanding how GenAI tools work, including their benefits, risks, limitations and biases;
- using GenAI tools in ways that enhance their subject matter expertise, critical thinking and creativity;
- using GenAI tools in ways that preserve human agency and accountability for decision-making and communication;
- ensuring output used for feedback or assessment is critically evaluated, noting that the sole use of GenAI tools to allocate marks or grades to students is not permitted;
- disclosing the use of GenAI tools where they have been used in ways that may impact upon members of the School community;
- liaising with IT to ensure that any GenAI tool usage is via an approved service, tool or website, or to request approval for the use of a new GenAI tool;
- reporting any inadvertent or accidental sharing of personal or sensitive data with GenAI (see below); and
- supporting students to use GenAI in line with Academic Integrity Protocols (see supporting/related documents).

Students are responsible for:

- complying with the School’s Academic Integrity Protocols and TASC Academic Integrity Procedures for Folio Assessment;
- disclosing the use of Generative AI tools to produce content included in or referenced for school-related submissions or assessments; and
- seeking support from teachers or IT if they are unsure of the appropriateness of their AI use.

Privacy considerations

School staff must carefully consider the data being shared with GenAI tools. Sharing personal or sensitive information belonging to staff, students or community members could lead to a breach of the School’s privacy obligations under the Australian Privacy Principles (APPs) as outlined in the Privacy Act 1988 (The Act). Generative AI tools should be considered unregulated third-parties unless they have been explicitly provided by the School (and its IT team) as internal resources, and their use must never compromise data security.

Personal information that can be linked back to an individual must never be used in Generative AI prompts, nor uploaded to or shared with online Generative AI tools, as such information will breach the School’s privacy obligations under the Act.

Records management and data retention

Staff must be careful when using Generative AI output for school-related work. Any data generated by an AI must be compliant with the School's Records Management Policy and Procedure. Where data is generated through a prompt that contains sensitive information (which is permissible, but only where that data has first been de-identified), it must be handled (and retained) in accordance with the School's Cyber Security Policy, Records Management Policy and Privacy Policy.

Approval and purchasing of access to Generative AI tools

Staff are welcome to use any GenAI tool provided that the information supplied to it (via a prompt) does not contain any personal or sensitive information that may be linked back to an individual. Some tools may be explicitly approved by the School for use; however, this does not equate to sponsorship. Financial costs associated with the use of GenAI tools rest with the user except where the School has already made a specific provision for finance.

Incident reporting and privacy breach protocol

Where staff become aware that personal or identifiable sensitive data has accidentally been shared with a Generative AI tool, they must immediately report the incident to the School's privacy officer at privacyofficer@hutchins.tas.edu.au.

Ongoing review

The School's IT team will monitor the use of Generative AI to support compliance with The Privacy Act, the Australian Privacy Principles (APPs) and School policies.

5. Supporting/related documents

Academic Integrity Protocols

Assessment and Reporting Guidelines

Safeguarding Australian Childhood Foundation Safeguarding Chidlren Program: Standard 1.4

Australian Framework for Generative Artificial Intelligence in Schools

ICT User Agreements

National Principles for Child Safe Organisations: Principles 8 and 10

TASC Academic Integrity Policy

6. Record keeping

This guideline is to be kept for three (3) years until review except where significant legislative or organisational change demands otherwise.

The master copy is kept in SharePoint Online in read-only PDF form. Printed copies are uncontrolled.

7. Guideline owner

The Principal

8. Version Control

Version Number	Author	Purpose/Change	Date
1.0	Head of Teaching and Learning (6-12) & Policy & Compliance Manager.	Initial release.	01/03/2025

Appendix A:
Staff GenAI Usage Expectations

All staff must adhere to the following expectations. While their primary focus is for staff, similar principles apply for students. The use of GenAI tools brings risk in respect to privacy and security. Where a staff member or student is unsure of their GenAI usage or its ethical implications, they should speak with the IT team for support.

You must not:

- **Upload private, sensitive or identifiable data**
  Never upload sensitive or personal data belonging to staff, students or community members, such as:
  - Full names
  - Addresses
  - Contact details
  - Synergetic id numbers
  - Identifiable health/medical data
  - Identifiable religious affiliation
  - Identifiable sexual orientation
- **Upload protected intellectual property (IP):**
  Is the document you want to upload publicly available? If so, it's likely okay to use. If it's not, consider whether it's appropriate to share. Does it contain intellectual property that we wouldn't normally share with another school? If so, don't upload it. If you're unsure, ask IT.
- **Rely on AI-generated outputs without verification**
  Avoid directly using AI-generated content in assessments, feedback, or official communication without review. Work you produce should be in your 'voice' and consistent with your practice.
- **Use AI tools that bypass school policies**
  Never use unauthorised or unvetted AI tools that may conflict with the school's policies or IT agreements.
- **Encourage students to input personal information into AI**
  Discourage students from entering their own or others' personal data into AI tools.
- **Upload photos of staff or students**
  Never upload images of staff or students to AI-based tools.

You may, with caution (consult IT if unsure):

- **Upload de-identified data for analysis**
  If using AI for insights or summaries (e.g., generating reports), ensure all data is anonymised. IT support may assist.
- **Use AI for professional development or planning**
  You may use online AI tools for planning lessons and generating resources, provided that you meet the requirements listed above to anonymise any student data. This can help with planning and differentiation without compromising student data security.
- **Use AI tools requiring logins or integrations**
  AI tools integrated with Learning Management Systems (LMS) may require IT setup to align with security and compliance standards. Ensure any AI tools in your software are disclosed to IT.
- **Experiment with AI for student engagement**
  When exploring AI tools for interactive learning or engagement, consult IT to confirm the tool complies with school-approved platforms.
- **Implement AI-driven classroom solutions**
  If introducing AI for classroom management or assessment (e.g., automated grading tools), ensure these are reviewed for alignment with privacy and quality standards.

You may:

- **Use AI for brainstorming or lesson planning:** Generate lesson ideas, adapt teaching strategies, or develop engaging classroom activities.
- **Create teaching resources:** Develop quizzes, summaries, or visuals that support lesson objectives.
- **Assist with administrative tasks**: Automate repetitive tasks like formatting documents, summarizing meeting notes, or scheduling.
- **Draft communication:** Use AI to draft emails, parent newsletters, or announcements, ensuring sensitive content is reviewed before sharing.
- **Research teaching strategies:** Leverage AI to find innovative teaching techniques, approaches, or resources.
- **Encourage critical thinking about AI:** Use AI-generated content in lessons as a teaching tool to develop students' analytical and evaluative skills.