TKIS Cyber Security and AI Use Policy and Procedures

PURPOSE OF POLICY

At the Kooralbyn International School (TKIS) we are committed to fostering a safe, respectful and responsible digital environment for students.

This policy promotes the responsible and educational use of Information and Communication Technology (ICT) resources, ensuring secure access to these services to enhance students' educational experiences. Parents and carers are expected to support their child's safe and responsible use of ICT resources, in line with this policy. Compliance with this policy is essential, along with adherence to the TKIS Student Anti-Bullying Policy, TKIS Student Code of Conduct and TKIS Mobile Phone Policy.

Responsibility

The Principal is responsible to the School Governing Body for the continuous monitoring and review of the Cyber Security and AI Use Policy and Procedures.

Point of Contact

Principal

SCOPE

This policy applies to:

- All students (including boarding students)
- All staff
- Contractors, volunteers, and visitors
- All devices (school-owned and BYOD)

DEFINITIONS

Artificial Intelligence (AI) - refers to software programs or platforms capable of performing tasks that typically require human intelligence. Examples include, but are not limited to AI writing tools (e.g., Grammarly, Microsoft CoPilot, use.AI), image generators, music production platforms, language translators, voice assistants, and data analysis software.

Cyber Security - Protection of systems and data from unauthorised access or attack.

Sensitive Information - Confidential or personal information relating to students, staff, or the school.

ICT Resources - Refers to electronic devices, internet services, school network systems, email services and digital tools provided by TKIS.

POLICY

The Principal is responsible for establishing policies and procedures to ensure AI is used ethically, responsibly, and in a manner that supports learning, critical thinking, academic integrity, and digital citizenship.

TKIS Cyber Security and AI Use Policy is collaboratively developed by the Senior Leadership Team in alignment with the Department of Education's policies and guidelines. TKIS currently uses Endpoint protection to safeguard against cyber threats, while also monitoring and providing weekly reports on student and staff activity. In addition, the PULSE wellbeing platform is being implemented, offering a live feed of student activity. PULSE identifies specific keywords and sends alerts to the management team and IT department when triggered.

The school requires all users to engage with ICT resources and AI in a safe, ethical, and responsible manner that protects individuals and the school community.

All students enrolled at TKIS who access or use AI tools and platforms are required to adhere to the TKIS Cyber Security and AI use Policy and Procedures, both at school and during school-related activities or assignments conducted at home or online.

PRINCIPLES

TKIS is committed to:

- Encouraging the ethical and informed use of AI in learning.
- Supporting students to develop digital literacy and critical evaluation skills.
- Protecting academic integrity and preventing misuse of AI for dishonest purposes.
- Ensuring student safety and privacy in digital environments.

RESPONSIBILITIES AND REQUIREMENTS FOR AI USERS

1. Teacher responsibilities

Teaching staff will:

- Be clear – verbally and/or in writing - when the use of AI is appropriate for a specific task or activity in class.
- Guide students to use sources of AI technologies that are safe and appropriate
- Actively monitor student progress during the development of written tasks or activities.
- Model responsible use of AI platforms to better inform student use.
- Seek approval from the Leadership Team before introducing new AI tools.
- All staff are required to undertake training in the use of AI platforms to:
    a) assist with the construction of activities and lessons
    b) provide guidance to students on responsible and educational use of AI.

2. Student responsibilities

Students will:

- Appropriately reference or declare the use of AI in the generation of works for their classes
- Follow teacher instructions for AI use.
- Follow academic integrity rules.

- Report misuse or unsafe behavior.
- Undertake school based AI use training.

Boarding students will:

- Follow device usage rules
- Use the internet responsibly
- Respect others' privacy
- Use ICT services only under adult direction and for learning-related purposes

3. Cyber Security Requirements

3.1 Access and Authentication:

- Use strong, unique passwords,
- Do not share login details
- Change passwords if compromised
- Use multi-factor authentication where available
- Log out of shared devices
- Update passwords quarterly (every term)

3.2 Users must not:

- Bypass school security systems
- Access inappropriate or illegal content
- Install unauthorised software

3.3 Data Protection

- Only access data for legitimate purposes
- Do not upload personal data to unauthorised platforms
- Follow school privacy requirements

3.4 Device Security

- Keep devices updated
- Use antivirus software
- Report lost or stolen devices immediately

3.5 Incident Reporting

All cyber incidents, suspected or observed, must be reported immediately to TKIS IT Department or school leadership.

PROCEDURES

Acceptable Use Guidelines

Students may use AI tools:

- To support learning under teacher guidance (e.g., brainstorming, researching, checking grammar).
- To enhance understanding of subject content.

- As part of approved classroom activities or assignments with teacher consent.
- To develop responsible digital practices.
- To support the development of human responses to specified instrument devices

Unacceptable Use Guidelines

Students must not:

- Submit AI-generated content as their own original work without acknowledgment.
- Use AI tools to cheat, plagiarise, or misrepresent understanding or effort.
- Use AI to produce inappropriate, harmful, offensive, or misleading content.
- Share or publish AI-generated content in a way that breaches school values or Department of Education guidelines.
- Use AI to bypass security, access restricted sites, or interfere with school systems.
- Impersonate others.
- Upload sensitive or personal data into AI tools.

Academic Integrity and Attribution

- Students must clearly acknowledge any substantial use of AI in assessments or assignments, following teacher or departmental guidelines (e.g., "AI tools were used to help generate ideas or summarise information").
- Teachers may require students to submit drafts, notes, or verbal explanations to verify understanding.
- Breaches of academic integrity due to misuse of AI will be treated seriously and managed in line with the TKIS' Assessment and Behaviour Management Policies.

Privacy and Data Protection

Students should:

- Avoid entering personal or sensitive information into AI tools.
- Understand that some AI platforms may store user data; therefore, school-approved or teacher-recommended tools should be prioritised.
- Three platforms are available for students to use: *Grammarly, Microsoft CoPilot, Use.AI*
- Seek permission before using AI tools not endorsed by the school.

Teacher Guidance and Monitoring

- Teachers will provide explicit guidance when AI use is permitted or encouraged for an activity.
- Staff will educate students about the capabilities and limitations of AI tools.
- AI use will be monitored, and any misuse will be addressed through existing pastoral care and behaviour processes.

Breaches of Policy

According to the Queensland Curriculum and Assessment Authority (QCAA), inappropriate use of AI (academic misconduct) can have several consequences and implications for students. These affect assessment results, certification, and future opportunities. Consequences may include:

- Parts of the assessment may not be marked if they are suspected to be dishonest.
- Only the sections proven to be the student's own work may be graded.
- If there is no authentic work, the student may receive NR (Not Rated) for that task.
- Re-submission of work.
- Loss of access to school technology resources.
- Disciplinary action in accordance with the TKIS' Behaviour Management Policy.
- Communication with parents/carers.

In any instance where a teacher has formed the belief that a student has used AI in an inappropriate manner (i.e. to falsely claim work as their own, to create inappropriate materials or other such actions) the following procedures will be followed (as per TKIS Assessment Policy):

First Occasion

- The teacher will inform the Head of Department or the Curriculum Coordinator and the student will be reprimanded by the class teacher.
- At the discretion of the teacher and/or Head of Department, one of the following consequences may apply:
  - The student may be required to re-submit the task, with a maximum mark of 50%. Further academic penalties may apply in accordance with the school's Assessment Policy,
  - An academic penalty based on the percentage of work AI generated,
  - A mark of 0 for the task.
- Parents/caregivers will be notified of the breach, and the outcome (what penalty has been applied).
- The teacher will record the instance as an 'E-Breach' on TASS

Second Occasion

- After discussion with the Curriculum Coordinator or HOSS, the student will be reprimanded by the class teacher and/or the Curriculum Coordinator. Parents/caregivers will also be contacted.
- At the discretion of the teacher and/or the Curriculum Coordinator, one of the following consequences may apply:
  - The student may be required to re-submit the task, with a maximum mark of 50%. Further academic penalties may apply in accordance with the TKIS Assessment Policy,
  - An academic penalty based on the percentage of work AI generated,
  - A mark of 0 for the task.
- The student may be required to complete future tasks by hand (i.e. without the use of a computer, and under the supervision of the teacher).

COMMUNICATION

This Policy is available to all staff, students, volunteers, contractors and TKIS community via the TKIS website. In addition, relevant aspects of this Policy will be raised at staff meetings and student Assemblies.

POLICY RELEASE DETAILS

Review Date: Annually

Next Review: February 2027

Approved by Principal

Date: February 2026