Queen’s College

Artificial Intelligence (AI) Policy

Prepared by the IT Committee (Version: 17/9/2025)

CHAPTER 1
INTRODUCTION

1.1. Purpose

The purpose of this Artificial Intelligence (AI) Policy is to establish clear, ethical, and secure guidelines for the procurement, development, and use of AI technologies at Queen's College. This policy is designed to ensure that AI is used responsibly to enhance teaching, learning, and administration while protecting the personal data, privacy, and well-being of our students, staff, and the wider school community. It aims to align the use of AI with our school's educational objectives and the Data Stewardship Values of being **respectful, beneficial, and fair**.

1.2. Scope

This policy applies to all members of the school community, including all teaching and non-teaching staff, students, and any third-party contractors or visitors who use or access the school's IT systems. It covers all AI systems, including predictive and generative AI, whether they are procured from third-party vendors, developed in-house, or accessed via school or personal devices (BYOD).

1.3. Definitions

- **Artificial Intelligence (AI):** A family of technologies that mimic human intelligence to perform tasks, solve problems, make predictions, and generate content. This includes generative AI tools like chatbots and image generators.
- **AI System:** The substantive programme or application used by the school that employs AI models to assist in operations.
- **AI Supplier:** Any third-party developer or vendor providing AI solutions or services to the school.
- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Users:** All individuals with access to the school’s IT and AI systems, including staff and students.

CHAPTER 2
AI GOVERNANCE AND PRINCIPLES

2.1 Ethical AI Principles

Our school is committed to the responsible and ethical use of AI, guided by seven internationally recognised principles:

1. **Accountability:** We are responsible for the AI systems we implement and their outcomes.
2. **Human Oversight:** The level of human involvement will be proportionate to the risks of the AI system, with the option for human intervention always available for high-risk applications.
3. **Transparency and Interpretability:** We will be transparent about our use of AI and strive to ensure that AI-assisted decisions are understandable.
4. **Privacy:** The protection of personal data is paramount. We will comply with the Personal Data (Privacy) Ordinance (PDPO) in all AI-related activities.
5. **Fairness:** AI systems will be used in a way that avoids unjust bias and unlawful discrimination.
6. **Beneficience:** AI will be used to benefit our students, staff, and community, while measures will be taken to prevent and minimise harm.
7. **Reliability, Robustness, and Security:** AI systems must operate reliably and be secured against errors and malicious attacks.

2.2. AI Governance Committee

To ensure adherence to these principles, the school has established an **AI Governance Committee** as a branch of the school's IT Committee.

- **Composition and Roles:**
    - The committee is led by the **Assistant Principal** and includes the **two IT Coordinators**.
    - The Principal will act as an advisor to the Committee.
    - The **IT Coordinator (Operations and Security)** is responsible for executing the policies of this committee in collaboration with all **KLA (Key Learning Area) Coordinators**.
    - The school's **Technical Support Staff** will provide frontline assistance to users, manage account access for approved tools, and handle initial troubleshooting for any technical issues related to AI systems.
- **Responsibilities:**
    - The committee is responsible for:
        - Developing and reviewing the school's AI strategy and this policy.
        - Overseeing the risk assessment and procurement process for all new AI systems.
        - Periodically reviewing approved AI tools for evidence of harmful bias and ensuring they are equitable and accessible for all students.
        - Ensuring adequate staff training on the responsible use of AI.
        - Reviewing AI-related incidents and ensuring a timely response.

CHAPTER 3

RISK ASSESSMENT AND HUMAN OVERSIGHT

3.1. Risk-Based Approach

The school adopts a risk-based approach to the management and use of AI systems. Before any AI system is procured or deployed, the AI Governance Committee will oversee a comprehensive risk assessment to identify and evaluate potential privacy, ethical, and security risks.

The assessment will consider factors such as:

- The **volume and sensitivity of personal data** involved (e.g., student health or performance data).
- The **potential impact** of the AI system's output on individuals (e.g., AI-assisted grading, or student support recommendations).
- The **quality and representativeness of the data** used to train or customise the AI, to mitigate the risk of unfair bias.
- The **security of the AI system** against unauthorised access or malicious attacks.

3.2. Levels of Human Oversight

Based on the risk assessment, an appropriate level of human oversight will be implemented.

- **High-Risk Systems** (e.g., AI for assessing student eligibility for activities): A **"human-in-the-loop"** approach will be used, where a staff member retains full control over the final decision.
- **Medium-Risk Systems** (e.g., AI for recommending learning resources): A **"human-in-command"** approach will apply, where staff oversee the AI's operation and can intervene or override its suggestions as needed.
- **Low-Risk Systems** (e.g., a library chatbot answering factual queries): A **"human-out-of-the-loop"** approach may be acceptable, allowing for full automation.

CHAPTER 4
PROCUREMENT AND USE OF AI SYSTEMS

4.1. Approved AI Tools

The AI Governance Committee will maintain an up-to-date list of approved AI tools and services. The current approved list includes:

- **Google Gemini (Using School Accounts only)**
- **Microsoft Copilot (Using School Accounts only)**

Staff and students are prohibited from using unapproved AI tools for storing, processing, or generating school-related data, especially personal or confidential information.

4.2. Third-Party AI Suppliers

When procuring AI solutions, the school will:

- Conduct due diligence to evaluate the supplier's competence, reputation, and commitment to security and data protection.
- Ensure that contracts include clear clauses on data protection, confidentiality, security requirements, and breach notification responsibilities.
- Verify that the supplier's practices align with the school's ethical principles.

4.3. Acceptable and Unacceptable Use

For All Users:

- **Do Not Share Sensitive Data:** Never input personal data (your own or others'), confidential school information, or proprietary material into public or unapproved generative AI tools.
- **Verify Information:** Always fact-check and verify the accuracy of information generated by AI, as it may be inaccurate, incomplete, or biased.
- **Respect Intellectual Property:** Do not use AI to create content that infringes on copyright or academic integrity policies. Properly attribute sources where required.
- **Report Concerns:** Promptly report any biased, harmful, or inappropriate output generated by an AI tool to the **IT Coordinators or the Technical Support Staff**.

Specific Prohibitions for All Users:
The use of any AI tool for the following purposes is strictly forbidden:

- **Misrepresentation:** Creating "deepfakes" or using AI to generate realistic but fake images, videos, or audio to impersonate or misrepresent any person (staff, student, or public figure).
- **Malicious Activities:** Generating malicious content, including phishing emails, harmful code, bullying, discriminatory remarks, or hate speech.
- **Illegal or Unethical Acts:** Any activity that violates the law, the EDB or school’s code of conduct, or academic integrity policies.

For Teaching Staff:

- **Professional Responsibility:** Teaching staff may use approved AI tools for work-related tasks, including lesson planning, creating educational materials, and administrative automation.
- **Human Review:** Staff must act as "human reviewers," carefully checking AI-generated content to ensure it is accurate, appropriate, and aligns with the school's pedagogical and ethical standards before sharing it with students or parents.
- **Confidentiality:** Uphold strict confidentiality of all student and school data. Use anonymised data whenever possible if using AI for analysis or content generation.
- **Guidance for Student Use:** To ensure clarity and fairness, teaching staff are required to explicitly state the rules for AI use for each assignment, task, or for their subject as a whole. This guidance must be clearly communicated to students and should specify the extent to which approved AI tools are permitted.

For Non-Teaching Staff (Administrative and Support):

- **Professional Responsibility:** Non-teaching staff may use approved AI tools to support administrative tasks, automate workflows, and enhance productivity.
- **Data Confidentiality:** All Non-teaching staff must adhere to strict confidentiality protocols. Sensitive administrative, financial, or personal data must not be inputted into any AI tool without explicit permission from the AI Governance Committee.
- **Verification of Output:** Information generated by AI for administrative purposes (e.g., summaries of documents, drafting communications) must be carefully verified for accuracy before being used or disseminated.

For Technical Support Staff:

- **User Support:** Provide frontline technical assistance to staff and students for all approved AI tools.
- **Account Management:** Manage user accounts, permissions, and access controls for school-sanctioned AI platforms.
- **Issue Escalation:** Escalate complex technical problems, security concerns, or reported policy violations to the IT Coordinators for further action.

For Students:

- **Permitted Use:** The use of AI tools by students is **prohibited by default**. Teachers may grant explicit permission for students to use approved AI tools for specific learning activities or assignments.
- **Academic Integrity and Declaration:** When AI use is permitted, students must not present AI-generated work as their own. Students are required to declare their use of AI when submitting assignments. Teachers will provide a designated space or format for this declaration.
- **Strict Prohibition in Assessments:** The use of any AI tool is **completely forbidden in all examinations, uniform tests and quizzes.**
- **Digital Citizenship:** Use AI tools respectfully and responsibly. Do not use AI to create harmful content, spread misinformation, or engage in cyberbullying.

CHAPTER 5
DATA PROTECTION AND SECURITY

- **Data Minimisation:** The school will ensure that only the minimum amount of personal data necessary is used for customising or operating AI systems. Anonymised or synthetic data will be used where feasible.
- **Data Security:** Robust technical and procedural controls will be implemented to protect AI systems and the data they process from security threats, including unauthorised access, data poisoning, and adversarial attacks.
- **User Privacy Settings:** Users should adjust privacy settings within approved AI tools where possible to prevent their data from being used for model training.
- **Secure Credentials:** Users must use strong, unique passwords where available for all accounts related to AI services. Users are strongly encouraged to enable multi-factor authentication (MFA) for all these accounts.
- **Data Handling:** All data inputted into and generated by AI systems must be handled in accordance with the school's Data Protection Policy and the requirements of the Personal Data (Privacy) Ordinance.

CHAPTER 6
TRANSPARENCY AND INCIDENT MANAGEMENT

6.1. Communication with Stakeholders

The school is committed to transparency. We will clearly disclose the use of significant AI systems to the relevant stakeholders (staff, students, and parents) and provide adequate information about their purpose, function, and potential impact. For high-risk AI systems, channels will be available for individuals to request explanations and human review of decisions.

6.2. Incident Response

Any user who suspects an AI-related incident—such as a data breach, the generation of harmful content, or a serious system error—must immediately report it to the **IT Coordinators** (or through the Technical Support Staff). All incidents will be managed in strict accordance with the **Queen's College Information Security Incident Handling Plan**.

CHAPTER 7
STAFF PROFESSIONAL DEVELOPMENT

The school is committed to providing ongoing professional development for staff on the effective and ethical use of approved AI tools in education. Professional development sessions will cover topics such as:

- Understanding the capabilities and limitations of AI.
- Practical strategies for integrating AI into the curriculum.
- Prompt engineering and getting the best results from AI tools.
- Identifying AI-generated content and upholding academic integrity.
- Mitigating bias and ensuring equitable use of AI in the classroom.

CHAPTER 8
GUIDANCE FOR PARENTS AND GUARDIANS

Promoting responsible and ethical AI use is a shared responsibility between the school and home. We encourage parents and guardians to:

- Discuss this AI policy and its principles with their children.
- Foster an open dialogue about the benefits and risks of AI technology.
- Supervise their children's use of AI tools at home, reinforcing the importance of digital citizenship, data privacy, and academic honesty.

CHAPTER 9
POLICY COMMUNICATION AND ACKNOWLEDGEMENT

9.1. Communication Plan

This AI Policy and any subsequent updates will be communicated to the school community through multiple channels, including:

- School notices to parents/guardians
- Announcements during school assemblies
- Discussions at Parent-Teacher meetings
- Email distribution to all staff and students

9.2. Formal Acknowledgement

All staff and students are required to formally acknowledge that they have read, understood, and agree to abide by this Artificial Intelligence (AI) Policy. This acknowledgement will be managed and recorded by the school administration.

CHAPTER 10
POLICY VIOLATIONS AND REVIEW

10.1. Violations

Violations of this AI Policy will be taken seriously and may result in disciplinary action in accordance with the school's Code of Conduct.

10.2. Policy Review

This policy will be reviewed at least annually, or more frequently if there are significant changes in technology, regulations, or school operations, by the AI Governance Committee.

CHAPTER 11
REFERENCES

For a deeper understanding of the principles guiding this policy, all staff are encouraged to review the following documents from the Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong:

1. Checklist on Guidelines for the Use of Generative AI by Employees (2025);
2. Artificial Intelligence: Model Personal Data Protection Framework (2024);
3. Leaflet on “Artificial Intelligence: Model Personal Data Protection Framework” (2024);
4. 10 TIPS for Users of AI Chatbots (2023);
5. Guidance on the Ethical Development and Use of Artificial Intelligence (2021); and
6. Leaflet on “Guidance on the Ethical Development and Use of Artificial intelligence” (2021).