Privacy Policy

1. Purpose and Scope

1.1 Purpose

The activities of King's Own Institute (KOI) as a higher education provider require it to collect, store and use personal information relating to its students, staff, and external partners. KOI acknowledges its obligation with regards to the collection, storage, and use of this information under the *Privacy Act 1988*, the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and the *Australian Privacy Principles* (APPs), the *Privacy Amendment (Notifiable Data Breaches) Act 2017 and the Privacy and Other Legislation Amendment Bill 2024 (Cth)*. In addition, KOI is subject to the General Data Protection Regulation (GDPR) of the European Union.

This policy sets out KOI's commitment to protecting personal information and outlines KOI's privacy management plan. The policy establishes clear guidelines for the handling of personal information within the institution and ensures compliance with all relevant privacy legislation and regulations.

1.2 Scope

This policy applies to the management of all information collected and held by KOI. It encompasses all KOI staff, prospective and enrolled students, contractors, and partners who interact with or manage personal information within the institution.

- The policy specifically excludes personal information that falls into the following categories: information available in public publications,
- materials kept in libraries, art galleries or museums for reference, study, or exhibition purposes,
- public records available for public inspection, and
- archives as defined under the *Commonwealth Copyright Act 1968*.

2. Related Documents

This Policy should be read in conjunction with KOI's Documents and Records Control Policy, which provides additional guidance on the management and retention of institutional records and documentation. Together, these policies form a comprehensive framework for information management at KOI.

3. Definitions

Personal Information: Personal information refers to any information or opinion that would allow an individual to be identified, or any information relating to the person's study or work at KOI. This encompasses a wide range of data including names, phone numbers, email addresses, nationality, date of birth, educational history, enrolment history, physical characteristics, health records and staff or student identification numbers. The veracity or format of the information does not affect its classification as personal information.

Sensitive Information: Sensitive Information includes specific categories of personal information that require additional protection, such as information about an individual's race, religion, ethnic background, health records and banking details, or any other information that might impact on study or work and the services provided by KOI.

AI-Generated Information: This encompasses data generated through KOI-approved artificial intelligence tools and platforms, including but not limited to:

- Learning management system AI features
- KOI-sanctioned AI-powered administrative tools
- Institutional AI analytics systems
- Academic integrity checking systems

This information may include user prompts, interaction logs, and generated outputs that can be linked to individual users' identities. All AI-generated information is stored within KOI's secure institutional systems and is subject to the same privacy protections as other forms of personal information.

4. Policy

4.1 Collection of Personal Information

KOI collects personal information through various paper and electronic formats regarding its staff, students, and external clients. The collection process occurs through multiple channels and interactions with the institution. This includes when individuals lodge online enquiries, apply for admission either directly or through education agents, enrol in courses, or apply for academic considerations such as extensions or deferred examinations.

The institution also collects personal information when individuals apply for employment, attend interviews, communicate via email, or complete any forms relating to their study or work at KOI. All collection processes are conducted with appropriate privacy safeguards and in accordance with relevant legislation.

4.2 Storage and Access

Personal information management at KOI follows strict security protocols. All personal information is maintained either as hard copy files or electronic records within individual student or employee files. Hard copy documents are secured in a monitored environment during business hours and locked securely outside of these hours to prevent unauthorised access.

Electronic records are protected through password-controlled access systems, with permissions granted only to staff members who require access to perform their specific duties. KOI implements a rigorous access control system where staff members are only granted access to the personal information necessary for their role.

Students and staff members have the right to access their own files under supervision, ensuring transparency while maintaining security. This supervised access process allows individuals to verify their personal information while protecting the integrity of the records.

4.3 Use of Personal Information

KOI utilises personal information to fulfill its core functions as a registered higher education provider and to enhance the educational experience of its students. The institution uses this information to communicate important updates about subject outlines, assessments, and attendance requirements, and to assist students in achieving satisfactory academic progress.

Personal information helps KOI implement diversity and equity initiatives, including providing reasonable adjustments for students who require them. It is also essential for resolving issues, handling complaints and appeals, and investigating any allegations of misconduct when they arise.

The institution uses personal information for administrative purposes such as processing wages and benefits, organising non-academic activities, and gathering feedback on learning and teaching. As educational technology evolves, KOI also uses personal information to improve its educational services through the appropriate application of AI technologies.

4.4 Use of Generative AI Technologies

KOI recognises the growing role of artificial intelligence in education and administration. The institution is implementing a framework for management of GenAI that ensures:

- Clear disclosure of AI system use in institutional processes
- Explicit consent requirements for AI processing of personal information
- Regular privacy impact assessments for AI implementations
- Documentation of AI decision-making processes that affect individual rights or interests

This framework specifically addresses:

- Automated decision-making in admissions processes
- AI-assisted assessment and feedback systems
- Administrative process automation
- Data analytics and reporting.

KOI will provide clear notice to affected individuals when AI systems are used in processes that may impact their rights, benefits, or access to services. This includes:

- Admission decisions
- Academic progression assessments
- Access to support services
- Administrative determinations

All AI-related privacy practices are implemented in accordance with KOI's Use of GenAI Policy, which provides detailed guidelines for the appropriate use of AI technologies within the institution.

5. Principles

KOI's privacy management is guided by several core principles that ensure the ethical and secure handling of personal information. The institution prioritizes collecting information directly from individuals whenever possible, seeking permission for third-party collection except in emergencies or when legally required.

Privacy notices are provided before any collection of personal information, clearly explaining the purpose, and intended use of the information. The institution maintains strict security protocols through restricted access systems and uses personal information only for its intended purposes as communicated to individuals.

All privacy protection measures are designed to comply with relevant legislative requirements and are regularly reviewed to ensure their effectiveness and currency.

6. Roles and Responsibilities

CEO and President: Serves as KOI's Privacy Officer with overall responsibility for information privacy governance.

Operational Responsibilities:

- Student Data (Non-Academic): Admissions, Student Support and Marketing departments
- Education Agent Data: Marketing department
- Student Data (Academic): Academic department
- Staff Data: Human Resources and Payroll departments

- Financial Personal Information: Finance department (including staff, students, vendors, third-parties, suppliers, and education agent commission)
- Privacy Breach Management: Governance, Risk and Compliance department (including complaint investigations and OAIC liaison)

Director of Governance, Risk and Compliance: Oversees the privacy framework and manages privacy-related complaints and investigations.

Each operational unit is responsible for implementing privacy protection measures within their respective areas and ensuring compliance with this policy.

7. Associated Information

This policy operates within a comprehensive legislative framework that includes:

- the *Privacy Act 1988*,
- the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, and
- the *Australian Privacy Principles* (APPs).

Additional relevant legislation includes:

- the *Privacy Amendment (Notifiable Data Breaches) Act 2017*,
- the *Education Services for Overseas Students Act 2000* and its associated regulations, and
- the *Higher Education Support Act 2003*.
- *and the Privacy and Other Legislation Amendment Bill 2024 (Cth)*

The policy also aligns with:

- the *National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students 2018*,
- the *Higher Education Threshold Standards 2021*, and
- the *Social Security (Administration) Act 1999*.

These legislative instruments together provide the regulatory framework within which KOI's privacy policies and procedures operate.

Document Control

Policy title	Privacy Policy
Policy owner	CEO, Dean and President
Policy approver	AIBM Council
Policy version date	07 March 2025 Version 1.3
Date of approval	07 March 2025
Date of implementation	07 March 2025
Date of next review	07 March 2026
Changes in this version	Addressing the privacy implications of generative AI while also including changes to align with the Policy Management Policy which provides the framework for the development, review, approval and publication of policies, procedures, and guidelines. This policy now follows the standard and format set out in the Policy Management Policy to ensure this policy document is accessible, consistent, and current and appropriately approved.