Privacy Policy

1. Purpose and Scope

1.1 Purpose

King's Own Institute (KOI), operated by Australian Institute of Business and Management Pty Ltd (AIBM), is committed to lawful, fair, transparent and secure management of personal information. This Policy explains the categories of personal information KOI collects, why and how it handles that information, how individuals may exercise access and correction rights, and how privacy concerns and incidents are managed.

This Policy is designed to give effect to the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and the Notifiable Data Breaches (NDB) scheme, and to support the Higher Education Standards Framework (Threshold Standards) 2021 as amended by the Higher Education Standards Framework Amendment (Threshold Standards) Instrument 2026. The July 2026 amendments apply in stages: racism-related requirements from 1 January 2027 and governance-related requirements applicable to KOI from 1 July 2027.

1.2 Scope

This Policy applies to KOI's handling of personal information concerning prospective, current and former students, applicants, graduates, staff, contractors, education agents, visitors, complainants, partners, and other individuals. It applies across the Sydney and Newcastle campuses, online and blended delivery, remote work, outsourced services and KOI-approved technology systems. All staff and service providers handling KOI information must comply with this Policy and applicable contractual obligations.

Legal exclusions or exemptions are determined by the Privacy Act and other applicable law; an item is not exempt merely because it appears in a public source, library or archive. Employee records are managed consistently with the applicable statutory position, including any exemption that lawfully applies; KOI nevertheless expects appropriate confidentiality and security controls.

2. Related Documents

This Policy should be read with KOI's Documents and Records Control Policy, Complaints and Appeals Policy, Use of GenAI Policy, information security and access management arrangements, incident response processes, student management procedures and relevant contractual confidentiality requirements. In the event of inconsistency, applicable law prevails.

3. Definitions

- 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.
- Sensitive information: Personal information comprising categories specified by the Privacy Act, including health information, racial or ethnic origin, religious or philosophical beliefs, political opinions, sexual orientation or practices, criminal record and certain biometric information. Financial and banking details are personal information requiring protection but are not automatically "sensitive information" under the statutory definition.
- Privacy breach: An act or omission involving personal information that may contravene the Privacy Act, the APPs or this Policy.
- Eligible data breach: A data breach satisfying the statutory conditions for notification under the NDB scheme, including likely serious harm and no effective remedial action preventing that harm.
- Automated decision-making: Use of a computer program to make, or to perform an act substantially and directly related to making, a decision involving personal information; additional

policy disclosure requirements apply from 10 December 2026 where the decision could reasonably be expected to significantly affect an individual's rights or interests.

- Privacy Officer: The person formally designated under clause 6 to oversee institutional privacy governance and act as the principal privacy contact.

4. Policy

4.1 Personal information collected

Depending on the relationship and the lawful purpose, KOI may collect identity and contact details; nationality and citizenship; date of birth; identity and visa or immigration information; education, enrolment, assessment, attendance and progression records; disability and reasonable adjustment information; health and support documentation; complaint, misconduct and safety reports; employment and payroll details; financial and payment information; scholarship and graduate-award information; website, learning management and account activity logs; and correspondence, recordings or other information provided in interactions with KOI.

KOI will collect sensitive information only where permitted by law, including where requisite consent is obtained or another legal basis applies, and will restrict its use and access in light of the risk of harm. Individuals may deal with KOI anonymously or by pseudonym where lawful and practicable; identification will ordinarily be necessary for admission, enrolment, academic records, employment, visa compliance and formal decisions.

4.2 Collection and privacy notices

KOI collects information directly from individuals through applications, enrolment forms, learning platforms, employment processes, inquiries, surveys, complaints and communications, and may obtain information from authorised education agents, referees, placement providers, academic partners, government agencies or other authorised third parties. At or before collection, or as soon as practicable afterwards, KOI will provide a notice required by APP 5, including the purposes of collection, material consequences if information is not provided, usual disclosures, access and complaints processes, and any likely overseas disclosures.

4.3 Uses and disclosures

KOI uses and discloses personal information for teaching, admission and enrolment, academic progression, assessment, learning support, student welfare and safety, complaints and appeals, academic integrity, graduation and award verification, employment, payroll, billing, legal and regulatory compliance, institutional governance, risk management, service delivery and other reasonably related lawful purposes.

Information may be disclosed to government bodies and regulators where authorised or required, service providers operating for KOI, external reviewers and professional advisers bound by appropriate obligations, and third parties as consented to or otherwise permitted by law.

KOI will not disclose student personal contact details, including private mobile telephone numbers, to lecturers, other students or external parties merely because they request them. Access or disclosure requires a legitimate institutional purpose, authorisation and a lawful basis. Internal role-based access is not equivalent to unrestricted disclosure. Direct marketing, where undertaken, will comply with APP 7 and applicable communications legislation.

4.4 Overseas disclosures and third-party systems

KOI does not ordinarily disclose personal information to overseas recipients as part of its current operations. Should an overseas disclosure be proposed, KOI will assess the arrangement beforehand and comply with APP 8 and any applicable notification requirements.

The use of externally hosted systems will be assessed according to whether information is disclosed to an overseas recipient, including the practical access and control arrangements.

Before approving a new third-party arrangement involving personal information, the responsible business unit and IT must consider confidentiality, access controls, permitted use, data location and access, retention, incident reporting, and lawful return or destruction of information.

4.5 Security, storage, retention and disposal
KOI will take reasonable steps to protect personal information against misuse, interference, loss, and unauthorised access, modification or disclosure. Measures appropriate to risk include restricted role-based access, multi-factor authentication where supported, secure physical storage, encryption, audit logging, backup and recovery, staff training, vendor oversight and timely removal of access when no longer required.

Records are retained for periods required by law, regulator obligations, contractual requirements and KOI's approved retention schedule. Personal information no longer required for a lawful purpose will be destroyed or de-identified in accordance with APP 11.2, subject to lawful retention obligations. Security obligations apply equally to paper records, email, mobile devices, remote work and cloud environments.

4.6 Access and correction
Individuals may request access to, or correction of, personal information held by KOI by emailing privacy@koi.edu.au. KOI may verify identity before release, will respond within applicable statutory timeframes, will provide reasons for lawful refusals and explain available complaint mechanisms. Access is not automatically contingent on supervised viewing: access may be provided in an appropriate secure form, subject to applicable exceptions. If correction is refused, individuals may request that a statement of the disputed information be associated with the record as required by APP 13.

4.7 Confidentiality of sensitive reports and safety matters
Records relating to student grievances, racism, discrimination, gender-based violence, health, disability and other sensitive matters will be handled on a restricted need-to-know basis. KOI will support safe and accessible reporting and investigation, fairness to affected individuals, protection against victimisation and proportionate disclosure to investigators, authorised decision-makers and agencies as required. Privacy must not be used to obstruct a lawful safety response, procedural fairness or a mandatory report.

This clause supports the information-handling aspects of the Threshold Standards, including the existing student grievance and wellbeing provisions and the amended racism and governance provisions as they commence; substantive case management obligations remain governed by KOI's related policies.

4.8 Graduate verification
KOI may maintain a graduate verification process and, where lawful, disclose limited details such as a graduate's name, qualification and conferral date to verify an award. KOI will provide appropriate notice and consider privacy, security, identity and misuse risks before making any public register searchable. Requests for access and correction may be made to the Privacy Officer.

4.9 Generative AI and automated decision-making
KOI does not currently use automated systems to make decisions about individuals. Staff must not enter personal information into unapproved public AI tools or external model-training services. Any proposed AI or automated decision-making use involving personal information must first undergo an appropriate privacy, security and governance assessment.

If KOI introduces automated decision-making that meets the statutory threshold, KOI will update this Policy and relevant privacy notices to meet the transparency obligations under the Privacy Act, including those commencing on 10 December 2026. This clause does not imply that such systems are currently in use.

4.10 Privacy incidents and notifiable data breaches

All staff and service providers must promptly report suspected or actual privacy incidents to privacy@koi.edu.au and the relevant IT/security contact. The Privacy Officer coordinates assessment and compliance with the NDB scheme, with IT leading technical containment, investigation and remediation. If

KOI has reasonable grounds to suspect an eligible data breach, it will undertake a reasonable and expeditious assessment and take all reasonable steps to complete that assessment within 30 calendar days. Where an eligible data breach is established, KOI will make notifications to the OAIC and affected individuals as required by law, as soon as practicable. Findings, decisions, remedial action and improvements must be documented.

4.11 Privacy complaints

A person may complain about KOI's handling of personal information by emailing privacy@koi.edu.au, identifying the concern and relevant facts to the extent practicable. KOI will acknowledge and assess the complaint, maintain appropriate confidentiality, provide an impartial response within a reasonable timeframe (ordinarily aiming for 30 days), advise of any further internal avenue, and record corrective action.

Individuals may complain to the Office of the Australian Information Commissioner (OAIC), generally after raising the matter with KOI and allowing a reasonable opportunity to respond. Privacy complaints involving students may also engage KOI's Complaints and Appeals Policy, but the internal pathway must not restrict statutory rights.

5. Principles

Lawful, fair and transparent collection, use and disclosure, with data minimisation and appropriate notice.
Purpose limitation, restricted access and strengthened protections for sensitive information.
Accuracy, availability of access and correction, and record integrity.
Privacy and security by design, including risk assessment for new systems and services.
Accountability and documented oversight, with timely incident escalation and continuous improvement.
Respectful, non-discriminatory and confidential handling of student and staff complaints and safety information.

6. Roles and Responsibilities

- AIBM Council: Retains its governance oversight responsibilities under KOI's existing governance arrangements. This administrative revision does not of itself seek or record a new Council approval.
- CEO: Retains executive accountability for implementation, resourcing and institutional compliance, with escalation of material risks and breaches.
- Privacy Officer — Anurag Kanwar: Is KOI's designated Privacy Officer and principal contact at privacy@koi.edu.au. Oversees the privacy framework; provides advice and compliance reporting; coordinates access/correction requests and privacy complaints; coordinates NDB assessments and regulatory liaison; and works with IT and business owners on risk assessments and improvement actions. This oversight role does not transfer day-to-day system ownership or security operations from responsible operational functions.

- IT function: Owns and implements technical information-security controls, access administration, logging, system security, backup and recovery, incident containment and technical investigations; promptly provides information required by the Privacy Officer.
- Academic, Admissions, Student Services, Marketing, HR, Payroll and Finance: Remain accountable for lawful collection, accuracy, access, disclosure, retention and secure handling of the information in their operational custody.
- All personnel, education agents, suppliers and contractors: Must comply with applicable confidentiality, security, contractual and reporting requirements and promptly escalate suspected privacy incidents.

7. Associated Information and Legislative Framework

- Privacy Act 1988 (Cth), including Australian Privacy Principles and the Notifiable Data Breaches scheme.
- Privacy and Other Legislation Amendment Act 2024 (Cth), including the automated decision-making transparency provisions commencing 10 December 2026.
- Higher Education Standards Framework (Threshold Standards) 2021, as amended in July 2026; relevant domains include 2.3, 2.4, 6.2, 6.4, 6.5, 6.9, 6.11 and 7.3, according to their applicable commencement dates.
- Education Services for Overseas Students Act 2000 (Cth), National Code 2018, and applicable student record/reporting requirements.
- Higher Education Support Act 2003 (Cth), where applicable, and other relevant Commonwealth and State requirements.

Document Control

Policy title	Privacy Policy
Policy owner	Privacy Officer — Anurag Kanwar
Privacy contact	privacy@koi.edu.au
Policy approver	AIBM Council (original approval authority)
Policy version date	06 November 2026 — Version 1.4 (administrative revision)
Date of approval	07 March 2025 (Version 1.3; historical approval)
Date of implementation	06 November 2026 (administrative revision)
Date of next review	06 November 2027
Changes in this version	Updated privacy and information-handling requirements; designated Anurag Kanwar as Privacy Officer; confirmed dedicated privacy contact, no current automated decision-making and no routine overseas disclosures; refreshed legislative references. No new Council approval is represented by this revision.