



Documents and Records Control Policy

1. Purpose

The purpose of this policy is to provide a framework to ensure that full and accurate records are created, captured and managed for all activities of King's Own Institute (KOI), to the standard required by the State Records Act 1998 (NSW) (State Records Act) and the Privacy and Personal Information Protection Act 1998 (NSW). The standards applied are those of GDA23 – General retention and disposal authority: university records (2005).

This policy should be read in conjunction with the Privacy Policy and the Critical Incident Policy (with reference to IT disruption and data breaches).

2. Scope

This policy applies to all electronic, hard copy and hand-written records within KOI, including teaching materials kept by KOI and not available to the general public through KOI. KOI records are the physical property of KOI and not of the staff member who created them or received them. Note that “documents” and “records” are interchangeable terms within KOI in most instances and that both terms have the ordinary dictionary definitions.

This policy applies to all staff and contractors at KOI.

3. Confidential documents

Non-confidential documents

Some documents are not confidential. They may be public documents that are displayed within KOI or be created by KOI for general interest or consumption. They may be distributed in open areas, in pamphlet stands or sent to agents and other persons.

Such documents are not subject to the confidentiality or access process specified in this policy but might be subject to version control. In case of doubt reference should be made to the CEO and President.

Confidential documents

Confidential information is information that should not be disclosed outside KOI and in some cases is limited to specified members of KOI staff. This includes business arrangements, financial and personal information of staff and students.

KOI is subject to a number of statutory requirements on the disclosure of personal records and other information. Refer to the Privacy Policy for details.

In case of doubt, the decision as to whether or not a document is confidential should be referred to the CEO and President.

4. Access

Persons designated by the CEO and President have access to documents, including teaching materials, as required within their areas of operation.

Records that are classified as confidential must not be provided to external parties unless appropriately authorised by the CEO and President. Original records must not leave KOI's control; only copies may be provided to external parties upon approval (unless originals are required by law).



All staff members who have access to hard copies of documents or records or to the central computer system, operate and have access only within specified limited areas, as applicable to their positions. If access is controlled by passwords, staff members will be given access as required.

5. Creation of documents

KOI documents are any documents that carry the name of KOI.

Staff members have authority to develop, create and amend documents within their areas of responsibility.

- All marketing materials come within the general control of the Marketing Director and must be cleared by the Marketing Director for compliance.
- All teaching materials come within the general control of the Vice-President (Academic).

6. Document version control

Documents must be captured in an approved record-keeping system as soon as practicable to ensure a full and accurate record is stored and managed.

Staff are responsible for ensuring records created or received via personal devices or programs are captured in the KOI recordkeeping system.

Document control procedures are specified on significant documents (such as policies, procedures and subject outlines) to ensure that documents are reviewed regularly by authorised staff and updated to maintain currency.

Hard copy documents

Hard copies (not being computer-produced) if they require amendment, will be amended by replacing the old (whole or part) document by the new one with the new date in the footer.

If the document is only paper and not electronic, old copies are to be placed in an ARCHIVE box file in secure storage.

Electronic documents

Controlled documents are kept electronically and generally accessible within the permission restrictions of KOI staff members or official sources.

All documents must remain in the appropriate computer folder or sub-folders as appropriate. When a file is up-dated or amended, a sub-folder labelled *archive* is to be created within the same folder. The replaced document is to be moved into the *archive* folder and the new, amendment becomes the main document. Paper copies of electronic documents are to be removed, defaced and destroyed. All electronically-created control documents must have a footer containing the file-path and the date of the version.

DO NOT ENTER the date automatically, - it must be typed in, otherwise the date would be changed automatically whenever the file is opened.

The amended document is printed and distributed in accordance with its needs.

7. Storage, archiving, retention and retrieval



All KOI records must be kept for the minimum periods identified in the State Records Act. Minimum periods may be increased but not decreased.

Storage. All KOI documents will be kept in a safe place within KOI. Documents that have a high security rating, such as academic progress and attendance, and student files, will be kept away from the public areas, in lockable cabinets or walk-in safe areas.

Retention. All documents will be kept for at least six years. This policy will be reviewed annually.

Archiving. Electronic archiving will take place for all electronic documents. Electronic documents are immediately accessible. The policy will be reviewed annually.

Thirty years of storage. KOI will keep individual records for 30 years. The first disposals will be examined at the end of 2040, other than the student records specified below.

Student records

KOI will maintain up-to-date records of all enrolled students or all new students who have paid tuition fees along with acceptance of offer, in its Student Management System. KOI will collect all the relevant information as prescribed by s 21(2) of the ESOS Act.

KOI will request all students to confirm the currency of their contact and other details as recorded in its Student Management System, every trimester. If KOI is notified of the changes in the details captured as per other process or by the student, KOI will update the records to maintain currency.

Where a student does not provide a response to the request to confirm the contact details as per above, KOI Student Support Services should engage in all reasonable means to establish contact with the student. In cases where students are non-contactable by the Student Support Services, a welfare check should be initiated as per the Support for Students Policy.

KOI will keep the following records as a minimum, for at least six years from the date after which a student leaves KOI:

- Records of each accepted student who is enrolled or who has paid any course money.
- Each accepted student's current residential address (as supplied by the student).
- The amounts of course money paid by the student.
- Whether the amount was paid for the full course or part of the course.
- If the amount was for the full course, the duration of the course.
- If the amount was for part of the course, the duration of that part of the course.
- Copies of written agreements between KOI and the student.
- Any amounts payable to undertake the course that have not been paid.
- Each accepted student's academic performance for each requirement of the student's course.
- Records of requests from students for a release and the assessment and decision on the request.
- Records of requests for deferment or suspension of study and the assessment and decision on the request.

8. Roles and responsibilities

The CEO and President has the responsibility of ensuring that KOI complies with the requirements for privacy and records.

The CEO and President is responsible for the implementation, monitoring and reporting on this policy. This includes developing a standardised records management system and assisting staff to establish and maintain records keeping systems.



The IT Manager is responsible for the security and back-up of IT systems and electronic records. This includes measures to prevent data breaches and the response and reporting on any such critical incidents.

All staff must

- create accurate records for all KOI activities in which they are responsible and all decisions which they take in the service of KOI
- maintain records in their custody in accordance with this policy
- protect confidential information in their custody from unauthorised access.

Document control

Policy title	Documents and Records Control Policy
Policy owner	CEO and President
Policy approver	Council, on recommendation of the Audit & Risk Committee
Version date	11 February 2024
Date of approval	1 March 2024
Date of Implementation	1 March 2024
Date of next review	1 January 2027
Changes in this version	Section 7: update on management of student records Replace Registrar with CEO and President

KOI amends its policies periodically and printed copies of this document, either in part or whole, are considered as uncontrolled and should not be relied upon as the most current document. It is the responsibility of individuals printing the document to always refer to the KOI website for the current version.

*****END OF POLICY*****