Records Management Policy

Web Link	
Category	Policy
Version	1.0
Policy Contact	Director of Academic Programs
Approving Authority	Academic Governance Board
Endorsing Authority	Executive Leadership Capability Advisory Committee (ELCAC)
Approval Date	1.7.23
Effective Date	1.7.23
Review Date	1.7.26
Related Documents	Australian Federal Police National Guideline on Information Technology (IT) Security AFP Record Keeping Policy Privacy Act 1988 (Commonwealth) Privacy and Personal Information Protection Act 1998 (NSW) (the PPIP Act) Health Records and Information Privacy Act 2002 (NSW) (the HRIP Act) Public Records Act 2002 Right to Information Act 2009

1. Purpose

1.1 Information is valued by the Australian Institute of Police Management (AIPM) as a core strategic asset and all records and archives will be managed in accordance with the Australian Federal Police (AFP), Commonwealth and New South Wales (NSW) State legislation, and appropriate recordkeeping standards.

1.2 The Records Management Policy establishes a framework for the collection, storage and disposal, of information relating to the activities of the Higher Education Faculty in the AIPM. The Records Management Procedure provides guidelines for implementation of this Policy and the circumstances under which information may be released to interested parties.

2. Scope

2.1 This policy applies to all records created or received by the AIPM staff in pursuit of functions or responsibilities undertaken within the Higher Education Faculty.

3. Policy Principles

3.1 Records are captured in recordkeeping systems:

3.1.1 For business continuity, so that relevant past decisions and activity can be accessed as necessary.

3.1.2 For the protection of rights, the AIPM's own and its obligations to staff, students and others affected by its actions.

3.1.3 Accountability, so that scrutiny can be made of AIPM business by anyone so authorised.

3.2 The AIPM uses and maintains records in a variety of corporate information systems, including business enterprise systems and student learning management systems. The major records held by the AIPM are student files and copies of papers submitted during the conduct of a program/unit.

3.3 Personal information will only be collected that is needed to carry out the AIPM' s functions and activities and information will be handled in accordance with the Privacy Laws and other applicable data protection laws (refer Records Management Procedures, Section 4).

3.4 Records must accurately reflect the activities they document and include adequate contextual information for them to be meaningful.

3.5 The AIPM conducts its business as "digital by default", wherever possible, with records created and stored in digital format.

4. Policy Statements

Student Records

4.1 Data collected from students enrolled in the program allows the AIPM to provide education and professional development services to students and to monitor progression through their units/programs.

4.2 Client Services is responsible for record management relating to student records.

4.3 Records created or received by email or electronic documents held on personal computers must be incorporated into the recordkeeping system (refer Records Management Procedures, Section 3 for more detail).

4.4 Similarly, oral decisions and commitments should be recorded and incorporated into the recordkeeping system such as documented in a 'file note' incorporated into the relevant file.

4.5 The AIPM will document and record responses to formal complaints, allegations of misconduct and breaches of academic integrity. Records relating to disciplinary matters, complaints or appeals will be kept in a separate confidential file.

Record Keeping

4.6 Student results are retained, archived and are able to be retrieved for 30 years.

4.7 Many of the records and intellectual property of the AIPM are stored in digital format and are managed and stored in a digital environment. Information received and records created digitally are expected to be maintained in a digital format throughout their lifecycle. Hard copy records are only created when necessary to meet legislative requirements.

4.8 All electronic data are kept in accordance with the Australian Federal Police National Guideline on Information Technology (IT) Security. The policy applies to all persons

appointed, employed, engaged, seconded or otherwise attached to the AFP under the provisions of the Australian Federal Police Act 1979.

4.9 Privacy provisions apply and record keepers are bound by the AFP Privacy Policy including the Privacy Act 1988 (Commonwealth) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

4.10 The AIPM Records Retention and Disposal Schedule provides a guide on records storage and disposal timeframes. Records and student files are held in accordance with AFP Record Keeping Policy and the Archive Act 1983. Files are held on site for seven years and then moved to the Commonwealth Archive in Canberra.

4.11 Any student complaints about the collection, storage and dissemination of information must be made in compliance with the complaints provisions of the Grievances, Complaints and Appeals Policy.

4.12 Complaints or potential breaches relating to research related information will be managed in accordance with the processes set out in the Research and Scholarship Procedure with documentation maintained on corporate information management systems in a separate confidential file.

5. Definitions

Archive are records selected for long-term retention for their value beyond their immediate administrative purpose, such as for future business needs, accountability, evidence and research.

Disposal is the processes associated with the removal of records from a recordkeeping system by destruction, deletion or transfer (e.g. to archives) which are documented in disposal authorities.

Records refers to physical and digital records that are created whilst performing an Institute function or activity, including but not limited to paper based records; databases; emails; scanned documents; records created in collaboration sites such as (but not limited to) MS365-Teams, Sharepoint, document libraries and OneDrive; completed on-line forms; actioned workflows; records created in cloud based third party applications; microfilm; tape; photos; video footage; webpages; social media content; maps; and research data.

Records management refers to the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including people, processes, and systems used to capture and maintain evidence of and information about business activities and transactions in the form of records.

Retention period is the minimum period of time for which records should be kept to meet regulatory, business, audit, legal and financial requirements before they can be destroyed.

Staff includes all those involved in the design and delivery of a program at AIPM, such as Visiting Fellows, affiliates and guest lecturers.

The Privacy Act (1988) is the principal piece of Australian legislation protecting the handling of personal information about individuals. This involves the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector.

REVISION HISTORY				
Version	Endorsed By	Approved By	Approval Date	Description of changes
1.0				New document.