Records Management Policy

Policy Code: GOV-013 **Version:** 3.0 **Effective Date:** 18 March 2015

Purpose:

The purpose of this policy is to provide guidance and direction on the creation and management of information and records and to clarify staff responsibilities. The College is committed to establishing and maintaining information and records management practices that meet its business needs, accountability requirements and stakeholder expectations.

The benefits of compliance with this policy will be trusted information and records that are: well described, stored in known locations and accessible to staff and clients when needed.

Definition of "College" – *The Australian College of Natural Medicine Pty Ltd (ACNM) trades as Endeavour College of Natural Health, FIAFitnation, College of Natural Beauty and Wellnation. For the purpose of this policy, any reference to 'College' or 'the College' should be considered a reference to each or any of these respective trading names.*

Scope:

- All Campuses
- All Staff
- All Contractors

Policy Statement:

The College's information and records are a corporate asset, vital both for ongoing operations and in providing valuable evidence of business decisions, activities and transactions.

There is an expectation that the College will uphold the obligations for privacy and security of personal details of all students, staff, clinic clients and customers. The College is committed to creating, and keeping, and disposing of accurate and reliable records to meet this obligation.

The College will implement fit-for-purpose information and records management practices and systems to ensure the creation, storage, and disposal via effective maintenance and

protection of reliable records. All information and records management practices in the College are to be in accordance with this policy and its supporting procedures.

This policy applies to the College's staff and contractors, to all aspects of the College's business and all business information created and received. It covers information and records in all formats including documents, email, voice messages, memoranda, minutes, audio-visual materials and business system data. The policy also covers all business applications used to create, manage and store information and records including the official records management systems, email, websites, social media applications, databases and business information systems. This policy covers information and records created and managed in-house and off-site.

This policy is written within the context of the College's internal information and Information Governance Framework which is located with the Office of the CEO. This policy is supported by complementary policies and additional guidelines and procedures which are located at on The Source.

Legislation and Other Key Mandates

The College's information and records management strategy and framework documents cover the legal, regulatory and business context within which the College operates.

Government agency-specific legislative requirements for creating or keeping, or disposing particular information and records are detailed within the Further Information section of this policy.

Creation and Maintenance of Information and Records

Business information and records will be created and captured by everyone subject to this policy. Business information and records created should provide a reliable and accurate account of business decisions and actions. It must include all necessary information to support business needs including the names, dates and time, and other key information needed to capture the business context.

All business information and records created and received should be captured into endorsed information and records systems unless they can be disposed of under the Records Management for Temporary Records Policy (Normal Administrative Practice - NAP).

Record Types

There are four key types of records stored at the College:

- Confidential
- Active
- Vital
- Archival

File Types

The College uses a number of key file types including:

- **Business** – General, Legal, Compliance & Governance
- **Finance** – Banking, Creditors, Legal Agreements
- **Human Resources** – Permanent Staff, Contract Staff, Occupational Health and Safety, Business Agreements & Workers Compensation
- **Clinic** – Medico Legal Client Files
- **Student Academic & Services** – Exams, Assessments/Quizzes, Grievances and appeals, Advanced Standing records, Student Files & Academic Due Diligence.

Protective Classifications

Records may be categorised under a number of classifications to identify the level of security required around the record. The full list of these classifications can be found in the Information Governance Framework.

Two types of classification are particularly important to be identified early as they contain highly confidential information:

- **Restricted**
- **X-in-confidence** (may include: Staff-in-Confidence, Security-in-Confidence Commercial-in-Confidence and Audit-in-Confidence).

Protecting these vital records ensures that the College has in place:

1. Measures to prevent or minimise the impact of a disaster event, and
2. Recovery and restoration measures if a disaster does occur.

Systems Used to Maintain Information and Records

The College's primary information and records management system is the Electronic Document Records Management System (EDRMS), on the College's SharePoint intranet site The Source. Where possible, all incoming paper correspondence received by the organisation should be converted to digital format and saved into the EDRMS. In limited

circumstances, such as for particular security purposes, there may be a requirement for paper files to be created or for soft copy files to be located elsewhere. Please contact a member of the Information and Records Management Committee in these instances.

The following business and administrative databases and software applications are endorsed for the capture and storage of specific information and records. These include:

- Sharepoint (The Source)
- Filemaker Pro
- AMINO
- Wellnation
- EXONET

A full register of endorsed systems used to create or manage information and records can be found in the Information Governance Framework. These endorsed systems appropriately support information and records management processes such as creation and capture, storage, protection of integrity and authenticity, security, access and retention, destruction and transfer of information and records.

Corporate records must **not** be maintained in email folders, shared folders, personal drives or external storage media as these lack the necessary functionality to protect business information and records over time.

Non Temporary Records created when using social media applications or mobile devices may need to be captured into an endorsed system.

Access to Information and Records

Sharing corporate information within the College

Information and records are a corporate resource to which all staff may have access, except where the nature of the information requires restriction. Access restrictions should be imposed with due care and consideration to the protection of:

- individual staff
- client privacy
- sensitive material such as security classified or material with dissemination limiting markings, for example ‘X in Confidence’.

The College is responsible for ensuring that records remain accessible to people with appropriate authority for the College, for the designated retention period. The College also

has in place mechanisms to safeguard privacy and confidentiality and prevent unauthorised use or access to its records.

It is the expectation of the College that a member of staff will access only those files and records which are necessary for the proper fulfilment of the duties of that member of staff, or that they are lawfully requested to access.

To prevent unauthorised disclosure of information, access to current databases is restricted to authorised staff. All requests for data are to be made via the Data Request Form to be reviewed by the College's Information Privacy Officer.

When handling information, staff are reminded of their obligations under the APS Values and Code of Conduct, the *Crimes Act 1914* and Public Service Regulations.

Release of publicly available information

In accordance with the College's obligations under the Information Publication Scheme and in the spirit of open-government policies, access to publicly available information will be provided on the College's website. This is the responsibility of the Information Privacy Officer.

The public additionally have legislative rights to apply for access to information held by the College under the *Freedom of Information Act 1982* and the *Archives Act 1983*. These apply to all information held by the College, whether in officially endorsed records management systems or in personal stores such as email folders or shared and personal drives. Responses to applications for access under Freedom of Information legislation are the responsibility of the Information Privacy Officer. Responses to applications for access under the Archives Act are the responsibility of the National Archives of Australia.

Retention or Destruction

College records are destroyed when they reach the end of their required retention period set out in records authorities issued by the National Archives of Australia. Retention periods in records authorities take into account all business, legal and government requirements for the records. The College uses a number of general and agency-specific authorities to determine retention, destruction and transfer actions for its records including the publicly available Universities Retention Schedule, Retention and Disposal Schedule VET, General Retention and Disposal Authority, General Disposal Schedule. Further details on where these documents can be found is in the Further Information section of this document.

Some records can be destroyed in the normal course of business. These are records of a short-term, facilitative or transitory value that are destroyed as a 'Normal Administrative Practice'. Examples of such records include rough working notes, drafts not needed for future use or copies of records held for reference. The College follows the Normal Administrative Practice which has been approved by the National Archives of Australia and which further defines the use of Temporary Records (NAP) by staff. All staff are responsible for being familiar with the policy and be aware that unauthorised destruction not only risks penalties under the Archives Act but may expose the College to a range of risks.

Staff should not destroy records, other than in accordance with the Records Management for Temporary Records Policy, without the approval of the Information and Records Management Committee.

Records that can be considered for destruction using Records Management for Temporary Records Policy fall into five broad categories:

1. **Facilitative, transitory or short-term items** including appointment diaries, calendars, 'with compliments' slips, personal emails, listserv messages and emails in personal or shared drives, emails that have been captured into a corporate records management system
2. **Rough working papers and/or calculations**
3. **Drafts not intended for further use or reference** – whether in paper or electronic form – including reports, correspondence, addresses, speeches and planning documents that have minor edits for grammar and spelling and do not contain significant or substantial changes or annotations
4. **Copies of material retained for reference purposes only**
5. **Published material not included as part of the College's records**.

Transfer

At times certain records may be required to be transferred out of the custody of College. This occurs when records of archival value are no longer being actively used. In this instance the College will transfer those records to an offsite secure archiving facility (currently Recall). The College is still able to access records if a subsequent need arises to consult records located at the offsite facility. Another instance where records may be transferred is when records are affected by administrative change and are transferred to the inheriting agency as legacy records.

Roles and Responsibilities

All employees: All staff, including short-term contractors (e.g. contract academics), are responsible for the creation and management of information and records as defined by this policy.

Additional responsibilities for certain staff are listed below:

Chief Executive Officer (CEO): The CEO is ultimately responsible for the management of information and records within the College. The CEO promotes compliance with this policy, delegates to a senior executive officer the responsibility for the operational planning and supervision of information and records management in the organisation, and ensures the College's information and records program is adequately resourced.

Senior management: Directors and senior personnel are responsible for the visible support of, and adherence to, this policy by promoting a culture of compliant information and records management, contributing to the development of strategic documents such as the information and records management framework and strategy. A Director is to be appointed and equipped to undertake the role of the Information Privacy Officer.

Information and Records Management Committee: Under the leadership of the delegated senior executive, the Information and Records Management Committee is responsible for overseeing the management of information and records in this organisation consistent with the requirements described in the policy. This includes providing training, advice and general support to staff, creating, developing or acquiring and implementing information and records management products and tools, including systems to assist in the creation of complete and accurate records, developing and implementing strategies to enable sound records management practices, monitoring compliance with information and records management policies and directives and advising senior management of any risks associated with non-compliance.

Information Communication Technology (ICT) staff: ICT staff are responsible for maintaining the technology for the College's business information and records systems, including maintaining appropriate system accessibility, security and back up. ICT staff should ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy. ICT and information and records management staff have an important joint role in ensuring that systems support accountable and effective information and records management across the organisation.

Information Privacy Officer: The Information Privacy Officer provides advice on security policy and guidelines associated with the management of information.

Managers and supervisors: Managers and supervisors are responsible for ensuring staff, including contract staff, are aware of, and are supported to follow, the information and records management practices defined in this policy. They should advise the Information and Records Management Committee of any barriers to staff complying with this policy. They should also advise the unit of any changes in the business environment which would impact on information and records management requirements, such as new areas of business that need to be covered by a records authority.

Contract staff: Contract staff should create and manage records in accordance with this policy to the extent specified in their contract.

Communication and Training

The College will ensure this policy is communicated to staff and that training is provided on aspects of the policy. When conducting training, it will be up to date, scheduled regularly, and tailored to ensure it is meaningful to different workgroups within the College.

Monitoring and Review

This policy will be updated as needed if there are any changes in the business or regulatory environment. It is scheduled for a comprehensive review annually. This review will be initiated by the Chair of the Information and Records Management Committee and conducted by an internal committee of senior management.

Compliance with this policy will be monitored by the Information and Records Management Committee with support of Directors and senior members of staff.

Related Procedures:

Clinic Client FOI - Requests for Records Procedure.docx
Records Management Procedure - Physical

Definitions:

Active - Referred to frequently used records in the daily operations of the College which are accessed frequently and refer to daily transactions such as student records/ activities etc. All

Active records are considered 'Unclassified' i.e. records that do not contain classified information until otherwise classified.

Archival - Records of any classification, marked or identified as **"Archive"** are to be moved from general use and stored securely as per their protective classifications and are accessed only by use of the Archives register to control, document and evidence access

Confidential - Records which contain sensitive and or personal information. Access to these records is restricted to certain College employees for specified purposes such as Access and Equity Officers located upon each campus. This includes and applies to specific College procedures given to information marked as *For Official Use Only* or *For Office Use*.

NAP - 'Normal Administrative Practice'. Covers **Temporary Records** including rough working notes, drafts not needed for future use or copies of records held for reference.

Protective Classifications – i.e. 'Restricted' may be used for records that have restrictions applied by the Office of the CEO and relates to sensitive information relating to the governance and management of the enterprise.

Student – is an individual person who is formally enrolled to study at the College. The individual person is that who appears on the College's documents such as enrolment, admission and payment documents, and who is assigned an individual student ID.

Temporary Records - see NAP.

Vital - records are those records that are necessary for the continued operation of the College. They are the core set of records containing the information required to re-establish the operations of the organisation. They protect the assets and interests of the College, and its clients.

Further Information:

Related Policies:	Acceptable Usage Policy - Information Resources Clinic Client FOI - Requests for Records Policy Clinic Client Health Records Disposals Policy Disability and Special Needs Policy IT Disaster Recovery Policy Records Management for Temporary Records Policy (NAP) Privacy Policy Risk Management Framework Policy Student Records Policy
Benchmarking:	National Archives Of Australia Universities Retention Schedule Retention and Disposal Schedule HE & VET General Retention and Disposal Authority General Disposal Schedule ADFA Express
Supporting Research and Analysis:	See Related Legislation below
Related Documents:	Information Governance Framework IT Disaster Recovery Plan Merged Retention and Disposal Schedule Secure Document Storage Request Form Retention and Disposal Schedule - VET
Related Legislation:	Archives ACT 1983 Charter of Human Rights and Responsibilities Act 2006 (VIC) Electronic Transactions (Qld) Act 2001 Evidence Act 1977 Fair Work Act 2009 (Federal) Fair Work Regulations 2009 (Federal) Financial Administration and Audit Act 1977

Freedom of Information Act 1982 (Vic)

Freedom of Information Act 1991 (SA)

Freedom of Information Act 1992 (WA)

Health Records Act 2000 (VIC)

Health Records and Information Privacy Act 2002 (NSW)

Health Services (Conciliation and Review) Act 1995:

Information Privacy Act 2000 (VIC)

Information Privacy Act 2009 (QLD)

Judicial Review Act 1991

Privacy and Personal Information Protection Act 1998 (NSW)

Public Records Act 2002 (QLD)

Right to Information Act 2009 (QLD)

Standards

AS ISO 15489 Australian Standard Records Management Parts 1 and 2, Standards Australia, 2002

Information Standard 40: Recordkeeping (IS40)

Information Standard 41: Managing Technology-Dependent Records (IS41)

Information Standard 42: Information Privacy (IS42)

Financial Management Standard 1997

Information Standard 24: Policies for the Management of Information within Government (IS24)

Information Standard 31: Retention and Disposal of Government Information (IS31)

Guidelines: N/A

Policy Author:	Quality and Compliance Coordinator
Policy Owner:	Information Privacy Officer
Contact:	Jennifer Osborne, Director Student Retention and Systems Jennifer.osborne@endeavour.edu.au
Endorsed:	Chief Executive Officer 10/02/2015
Approval Body:	College Council
Policy Status:	Revised – fully reviewed
Responsibilities for Implementation:	Chief Executive Officer Chief Financial Officer Information Privacy Officer College Directors Senior Management All staff including contractors
Key Stakeholders:	Chief Executive Officer Chief Financial Officer Director Student Retention and Systems Director, IT & Learning Systems Support Director, Admissions and Marketing Director of Education Director – VET Operations Director, Aesthetics Education National Compliance Manager National Librarian