Marywood University
Policies and Procedures

Records Management Policy

Policy Statement:

1. Purpose

The purpose of this policy is to establish decentralized guidelines and procedures for the effective management of records and archives at Marywood University. This policy seeks to ensure that records are properly maintained, preserved, and accessible in accordance with legal and regulatory requirements, while also supporting the university's operational and strategic objectives.

2. Scope

This policy applies to all records, regardless of format or medium, created, received, maintained, or used by Marywood University, its employees, students, alumni, and donors. It encompasses both physical and electronic records.

3. Definitions

- Records: Any recorded information, regardless of physical form or characteristics, created or received by Marywood University in the course of its operations.
- Archives: Records that have been identified as having permanent historical, administrative, or legal value and are selected for long-term preservation and access.

4. Specific Departments of Impact

The university must comply with laws, rules and regulations concerning the retention of records. These laws, rules, and regulations are different for areas of the university, dependent on the area's status, purpose, and accreditations.

Departments commonly subject to legal retention requirements include:

- **Human Resources (HR) Department:** HR departments are usually required to retain records related to Title IX investigations, employee hiring, employment contracts, payroll records, performance evaluations, disciplinary actions, and termination documentation. These records are often subject to various federal, state, and local employment laws and regulations.
- **Admissions Office**: The Admission Office must comply with applicable federal regulations, including the Family Educational Rights and Privacy Act (FERPA) and the Higher Education Act (HEA). These laws govern the privacy and security of student records and may stipulate specific retention periods for admission-related documents.

- **Dean of Students**: The Dean of Students may need to retain a variety of documents related to student affairs, disciplinary matters, student services, and other administrative functions.
- **University Advancement:** University Advancement offices at universities typically handle fundraising, alumni relations, donor stewardship, and other development activities. Document retention requirements for such offices are crucial for maintaining transparency, accountability, and compliance with legal and ethical standards.
- **Registrar's Office:** The Registrar's Office typically maintains records related to student admissions, enrollment, academic transcripts, course registrations, and graduation certifications. These records may be subject to federal laws such as the Family Educational Rights and Privacy Act (FERPA), which governs the privacy of student education records.
- **Financial Aid Office:** The Financial Aid Office is responsible for maintaining records related to student financial aid applications, awards, disbursements, and loan agreements. These records are often subject to federal regulations such as the Higher Education Act and may have specific retention requirements outlined by the Department of Education.
- **Business Office:** The Fiscal Office maintains financial records, including budgets, financial statements, invoices, contracts, insurance policies, procurement documents, and student account records. These records are subject to various financial regulations and may need to be retained for auditing and compliance purposes.
- **Health Services, Counseling and Student Development Center/Counseling Center/Speech, Language and Audiology Clinics:** Departments providing health services or counseling to students may have legal requirements to retain records related to medical treatments, counseling sessions, health insurance, and confidentiality agreements. These records are subject to laws such as the Health Insurance Portability and Accountability Act (HIPAA) and state privacy laws.
- **Campus Safety:** Public safety or security departments may be required to retain records related to incident reports, crime logs, security camera footage, and investigations. These records are often subject to laws such as the Clery Act, which requires colleges and universities to disclose campus crime statistics and security policies.
- **Academic Affairs, Academic Departments/Faculty Offices:** Academic Affairs, academic departments and faculty offices may retain records related to accreditation, curriculum development, research projects, academic publications, faculty evaluations, and art collections. These records may be subject to institutional policies as well as professional standards and accreditation requirements.
- **Athletics and Recreation:** Athletic departments are subject to federal laws, including but not limited to FERPA and HIPAA, which may impact the types of records that must be retained and the duration for which they must be kept. Further, as a member of the National Collegiate Athletic Association (NCAA), the University's Athletics and Recreation department must also comply with NCAA standards or rules and regulations regarding all member institutions. These regulations may pertain to areas such as compliance, recruiting, eligibility, and financial aid for student-athletes. The NCAA Board of Governors, the highest-ranking committee in the Association, can implement policies by which all three divisions must abide.
- **Office of Institutional Equity and Inclusion and Title IX** - Title IX regulations require that records related to investigations, complaints, and compliance efforts must be maintained for a period of

seven years. Pennsylvania institutions must comply with federal laws and regulations, including Title IX of the Education Amendments Act of 1972 and associated regulations issued by the U.S. Department of Education's Office for Civil Rights (OCR).

It is essential for university departments to be knowledgeable regarding the specific legal requirements applicable to their department's records and to establish comprehensive records management procedures to ensure compliance with these obligations and this policy.

5. Responsibilities

- **Central Records Management Officer (RMO):** The Central RMO designated by the Vice President for Finance and Administration is responsible for establishing overarching policies, procedures, and guidelines for records management and archives. These policies and guidelines will provide guidance, support, and oversight to decentralized units and ensure compliance with legal and regulatory requirements.
- **Decentralized Units:** Each department or unit within the university is responsible for implementing and managing records within their respective areas. Department heads or designated records managers are responsible for ensuring compliance with this policy and coordinating with the Central RMO as needed.
- **Records Custodians:** Records custodians within decentralized units are responsible for the day-to-day management of records, including classification, organization, storage, and disposal, in accordance with established procedures and guidelines.
- **Information Technology (IT) Department:** The IT Department provides technical support and resources for the management of electronic records, including storage, backup, and security measures, in coordination with decentralized units. The university's IT Department must also ensure the security and privacy of stored documents, particularly those containing sensitive personal information. This requirement includes implementing safeguards against unauthorized access, data breaches, and other security risks.

6. Record Lifecyle Management

The management of records at Marywood University follows a decentralized lifecycle approach, with decentralized units responsible for the following stages:

- **Creation and Receipt:** Decentralized units ensure that records are created or received in the course of university activities, capturing necessary metadata associated with each record.
- **Classification and Organization:** Records are classified according to their content and importance within decentralized units, with appropriate retention and disposal schedules applied.
- **Storage and Security:** Decentralized units are responsible for storing records in secure facilities or electronic systems with appropriate access controls, backed up by support from the IT Department.

Retention and Disposal: Decentralized units adhere to the university's retention schedule, disposing of records securely at the end of their retention period in accordance with established procedures.

7. Records Management

Decentralized units collaborate with the Central RMO to manage records, with responsibilities including:

- **Appraisal and Selection**: Decentralized units collaborate with the Central RMO to identify records with archival value and in selecting materials for long-term preservation.
- **Arrangement and Description:** Decentralized units assist in arranging and describing records, ensuring adherence to generally accepted professional metadata standards.
- **Preservation and Conservation:** Decentralized units contribute to the preservation and conservation of records, following guidelines provided by the Central RMO.
- **Access and Use:** Decentralized units coordinate with the Central RMO to provide authorized users with access to records in accordance with applicable policies and procedures.

8. Compliance Monitoring

Decentralized units are responsible for ensuring compliance with this policy within their respective areas, with the Central RMO providing oversight and support.

The Central RMO must conduct periodic audits and reviews to ensure adherence to policy requirements.

9. Policy Review and Revision

The Central RMO reviews this policy periodically in collaboration with decentralized units to ensure its effectiveness and relevance.

10. Policy Communication and Training

All employees will be provided with a copy of this policy and any related procedures.

Training and awareness programs will be conducted to ensure understanding and compliance with this policy and associated practices within decentralized units.

11. Decentralized Policy Requirements

Each Decentralized Unit's internal policy must address the following items:

- Record Classification and Retention Periods: Specific document definitions and retention requirements.
    - Strongly recommended to include the legislative or regulatory resource that requires retention of the documents.
- Process and Procedures related to obtaining, retaining, and destroying documents.
- Record Disposal: Annual schedule for document destruction.

12. Document Control

This Records Management Policy is effective upon approval by the President of the University and supersedes any previous policies or guidelines on the subject matter.

Definitions:

- Records: Any recorded information, regardless of physical form or characteristics, created or received by Marywood University in the course of its operations.
- Archives: Records that have been identified as having permanent historical, administrative, or legal value and are selected for long-term preservation and access.

Policy History:

12/01/00 - Approved by the President as recommended by the Policy Committee of the University
11/04/05 - Revision approved by the President of the University as recommended by the Policy Committee of the University
05/10/2024- Revision and Title Change approved by the President of the University as recommended by the Policy Committee of the University.

Related Committees

Institutional Property Policy

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES

Mary Theresa Gardier Paterson, Esquire
Secretary of the University and General Counsel