



UNIVERSITY OF
WEST GEORGIA

Records Information Management Program Overview

Brief Description:

Records are a valuable university asset that provides evidence of decision-making and business activities, reduces risks from legal or regulatory challenges, reduces operational costs, and improves the efficiency and effectiveness of the Institution.

Office of Legal Affairs
1601 Maple Street, Carrollton, GA 30118
westga.edu
Revised January 2023

The University of West Georgia would like to acknowledge colleagues' work at other institutions and agencies.

This document was created and modified using the following sources:

DePaul University. (2016, October 1). Records Management Manual. Retrieved January 30, 2018, from http://rm.depaul.edu/Forms/DePaul_RM_Manual.pdf

Alaska State Libraries Archives & Museum. (2017, July). SOA Records & Information Management Service POLICIES AND PROCEDURES MANUAL. Retrieved January 30, 2018, from http://archives.alaska.gov/pdfs/records_management/manual/records_management_manual.pdf

Summary

Welcome to the University of West Georgia's Records Information Management (RIM) Program.

This document outlines the mission of the RIM program, the scope of service it provides, and general information about records information management for all university employees.

Below are the links to:

RIM homepage

<https://www.westga.edu/administration/president/legal/rim/index.php>

RIM Policy 1008 [Records Information Management](#) and associated procedures



Mission Statement

Our mission is to direct records information management initiatives that promote university-wide participation and accountability, to achieve compliance with State of Georgia Statutes, University Policies, and associated procedures while contributing to the preservation and advancement of the University of West Georgia (UWG).

The Chief Legal Officer (CLO) designates the Director of Policy and Information Management as the Records Management Officer (RMO) to oversee the RIM program

Goals and Objectives

The Records Information Management Program accomplishes this mission by:

Goal 1: Develop effective records information management strategies for the University of West Georgia

- Develop and implement an institutional RIM program for UWG;
- Develop and maintain the USG Records Retention Schedule as well as supplemental campus-based schedules and forms;
- Identify and take adequate steps to protect confidential and essential business (vital) university records.

Goal 2: Provide the framework for records information management education, awareness, and innovation across all levels of the organization

- Lead and guide the University in matters relating to records information management to fulfill the mission of the program and to help ensure compliance across the University;
- Promote sound records information management principles and initiatives and make recommendations regardless of format for best methods and systems for managing records;
- Provide timely information management training, communication, and awareness;
- Form strategic partnerships with USG System institutions, state agencies, and other organizations to create ongoing awareness, efficiency, and innovation.

Records Information Management Program

Records Management Policy and Procedures

The framework of the RIM program is its policy and associated procedures. Implementing the Records Retention and Disposition Schedules (RRDS) will help facilitate efficient recordkeeping and result in efficient space planning. The proper use of the RRDS will ensure the satisfaction of the University of West Georgia's legal and compliance requirements for managing records. The Office of Legal Affairs is the steward of this policy, ensuring its contents are relevant and timely as they relate to the University community.

Records Retention and Disposition Schedules (RRDS)

As a functional extension of the RIM Policy, the University of West Georgia adopted the University System of Georgia's (USG) Records Retention and Disposition Schedules. The schedules provide a description and retention period for known university records and are updated periodically with new records series and retention periods. The Office of the Governor and the Georgia Archives approves all RRDS entries.

Records Training Opportunities

With a solid commitment to education, the RIM Program offers training and information sessions on various topics by appointment.

Topics covered may include but are not limited to:

- Introduction to Records Management
- Disposing of University Records
- Completing a Records Inventory
- Georgia Open Records Act

Consultations

As another form of support, the RIM Program offers free consultations for departments wishing to improve RIM processes and/or grapple with unruly space environments.

File Storage and Destruction

Through an approved partnership, University has access to off-site records shredding and shred bins for interested departments.

Records Management Liaisons (RML)

Each department must designate one employee (maximum two) to serve as Records Management Liaison (RML). The University's Records Management Officer (RMO) will communicate with RMLs to ensure the message of records information management reaches the University community. RMLs and members of the University will receive updates on policy changes, training, and educational opportunities.

Table of Contents

SUMMARY	iii
MISSION STATEMENT	
GOALS AND OBJECTIVES	
Records Information Management Program.....	iv
Records Management Policy and Procedures	
Records Retention and Disposition Schedules (RRDS)	
Records Training Opportunities	
Consultations	
File Storage and Destruction	
Records Management Liaisons (RML)	
Section 1 Introduction	1
1.0 What is records information management (RIM)?	1
1.1 What are the five steps to managing records information through the lifecycle?	1
1.2 What are the benefits of records information management?	2
1.3 What is a record?	2
1.3.a What is an official record?	2
1.3.b What is an unofficial or non-record?	3
1.3.c Can an unofficial record become an official record?	3
1.4 Why is it essential to create and manage records?	3
Section 2 Records Retention and Disposition Schedules (RRDS).....	4
2.1 The organization of the Records Retention Schedules	4
2.2 Amending the Records Retention Schedules	4
Section 3 Implementing the Records Retention Schedules	5
3.1 Records Destruction	5
3.1.a Disposal of unofficial records and non-records	5
3.1.b Destruction of all other official records	5
3.1.b.1 Certificate of Destruction.....	5
3.1.b.2 Destruction Method.....	5
3.2 Transferring Records to University Special Collections	6
Section 4 Suspension of Retention Schedules	7
4.1 Initiation of Legal Holds	8
4.2 The Scope of Legal Holds	9
4.3 The Release of Legal Holds	9

Section 5 Records Confidentiality, Access, and Security	10
5.1 Records confidentiality and security	10
5.2 Records security	10
Section 6 Training	11
Section 7 Roles, Responsibilities, and Accountabilities.....	11
7.1 Data Owner (University President)	11
7.2 Data Trustees	11
7.3 Data Stewards.....	11
7.4 Chief Information Officer (CIO)/ Chief Information Security Officer (CISO)	11
7.5 Data Users	12
7.6 Information System Owner	12
7.7 Information Technology Services (ITS)	13
7.8 Chief Legal Officer (CLO).....	13
7.9 Office of Legal Affairs (OLA).....	13
7.10 University Records Management Officer (RMO).....	13
7.11 Records Management Liaisons (RML).....	13
7.12 Records Information Advisory Group	14
7.13 Third Parties	14
Section 8 Records Policies, Procedures, and Practices	15
<i>Appendix A - Vocabulary</i>	16

Section 1 Introduction

This overview guides University offices in defining their internal records procedures and serves as a foundation for establishing consistent and reliable university recordkeeping practices while ensuring the safety, security, and authenticity of the University of West Georgia records.

1.0 What is records information management (RIM)?

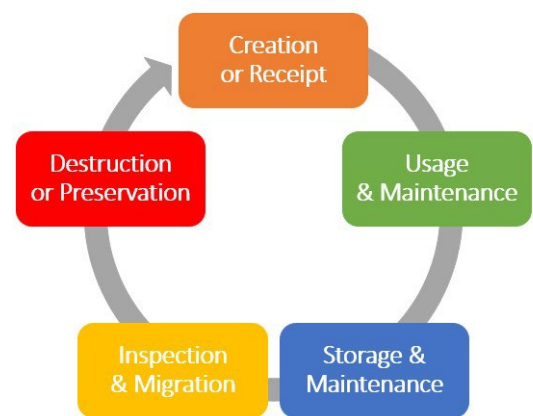
Records Information Management (RIM), also known as records management (RM), is the systematic control of all records (regardless of storage media/location) from creation or receipt through processing, distribution, use, retrieval, and maintenance to their ultimate disposition. The policies, procedures, and rules that govern the control of records comprise a RIM program.

A RIM program includes:

- Records management policies and procedures.
- Skilled staff.
- Recordkeeping systems and tools.
- Advice and training in records management.
- Records management performance monitoring and review.

Records Information Management addresses the lifecycle of records, i.e., the length of time records is in the custody of University offices. The lifecycle usually consists of five stages:

- Creation or Receipt.
- Usage and Maintenance.
- Storage and Maintenance.
- Inspection and Migration.
- Destruction or Preservation.



1.1 What are the five steps to managing records information through the lifecycle?

An integrated lifecycle approach denotes a consistent and coherent set of seamless management processes. The integrated records management lifecycle model requires data governance, shared accountability, and a commitment to information stewardship to ensure the sustainability of these critical management activities.

Step 1 Creation or Receipt:

When information and records are produced or received (and before creation, in the design of records systems) in various formats using different equipment and technologies.

Step 2 Usage and Maintenance:

When information and records are transmitted to those who need them and, upon receipt, are used to conduct university business. Records are filed or stored according to a logical scheme to permit subsequent retrieval, storage, protection, and maintenance to safeguard the integrity of the information. During this stage, the information is active; it is frequently referred to and thus usually stored close to its users.

Step 3 Storage and Maintenance:

When information and records decline in value, they become inactive. Records are then removed from active storage (i.e., prime office space) or transferred to inactive or off-site storage for retention life. Records are filed or stored according to a logical scheme to permit subsequent retrieval, protection, and maintenance to safeguard the integrity of the information. During this stage, the information is inactive; it is not frequently accessed.

Step 4 Inspection and Migration:

Migrated records should be verified, searchable, and retrievable after information and records are reviewed and shifted from one system, mode of operation, or enterprise to another.

Step 5 Destruction or Preservation:

When information and records reach the end of their retention period and have no further legal, fiscal, or administrative value, they are: (1) safely destroyed or (2) preserved permanently for ongoing historical reference or research purposes.

1.2 What are the benefits of records information management?

University offices create and maintain records as a by-product of conducting business that provides evidence of what happened, why, and by whom. They are valuable university assets that can improve the efficiency and effectiveness of university operations through their retention and reuse.

Records also support accountability, which means providing an explanation or justification and accepting responsibility for events or transactions. Accountability is internal and external to the university, including delegating responsibility to staff and reporting to outside entities.

A records management program provides:

- Volume reduction and cost control by reducing costs associated with storing records that have met their retention period.
- Access to information with improved records retrieval.
- Identifying records of continuing value to the university.
- Litigation risk management in minimizing discovery costs with prompt and accurate responses to litigation discovery requests.

1.3 What is a record?

A record is any recorded information, regardless of storage media or format, created, received, or maintained as evidence of conducting business. A record provides evidence of university activities and can be in any format or media, including paper, microfilm, and electronic.

Examples of records include:

- Official Records
- Contracts
- Unofficial Records
- Committee minutes
- Student applications
- Budgets
- Policies and Procedures
- Reports

1.3.a What is an official record?

An official record is the complete (final), authoritative version retained and required for business or legal reasons. Official records provide evidence of the University of West Georgia's organization, business activities, decisions, procedures, operations, and internal or external transactions and reflect the University's intent to preserve such information. Records are considered 'official' when they are in a final form and held by the designated "Office of Record."

Examples include:

- Records maintained in an employee's personnel file by Human Resources.
- University budget created and maintained by the Office of Budget.
- Student treatment records created and maintained by Health Services and the Counseling Center.
- Student transcripts maintained by the Registrar.

The "official retention period" identified in Records Retention Schedules for the University System of Georgia applies to Official Records. (*see Section 2 in the Records Information Management Program Overview*)

As part of the RIM Program, an *office of record* may be established for each records series to avoid duplication of holdings across departments and agencies. Only the identified *official record* is to be retained to comply with federal or state requirements or for permanent historical and research value. The Office of Record is responsible for managing, retaining, and the timely destruction of particular official University Records.

1.3.b What are unofficial or non-records?

Unofficial also referred to as non-records, have no legal or business requirements to be retained. These records are used for reference purposes and referred to as duplicates, convenience, transitory, drafts, or working papers. The differences between a non-record and an official record are the reasons for keeping the information and how the content is used.

The RIM policy does not pertain to non-records; therefore, these do not need to be retained, stored, disposed of, or destroyed following procedures created under this policy and state law. As soon as unofficial records have met their immediate business need, they may be discarded but never kept longer than the retention period for the office of record.

1.3.c Can an unofficial record become an official record?

In a legal proceeding, an unofficial record can be used in court. Lawful discovery requests may compel the production of any or all draft documents. To prevent the required production of unofficial records:

- Ensure that unofficial records are not kept longer than the retention period for the official record.
- Dispose of duplicate records when they are no longer useful.

1.4 Why is it essential to create and manage records?

Virtually every aspect of the university's business depends upon records. Some records are created automatically as a part of doing business. For example, when an email message is used to transact business, a record is created and should be retained as evidence of that business activity. Human Resources maintain employment applications as records to document an employment activity and to satisfy legal and regulatory retention requirements. Other transactional business activities routinely created include sending invoices, executing contracts, and issuing reports.

Other university activities may not routinely create records. For example, meetings of boards and committees do not automatically generate records; therefore, minutes are deliberately created and distributed to document board and committee actions. A record should be established for activities that do not result in the automatic creation of records.

Records can be created in any format and stored in various media. However, in today's work environment, most records are created electronically, stored digitally, and often printed. Hence university recordkeeping systems maintain records in various media, including paper, microfilm, optical media, and magnetic tape.

Creating and maintaining complete and accurate records to provide credible evidence of university decisions is essential.

Section 2 Records Retention and Disposition Schedules

The University of West Georgia's Records Retention and Disposition Schedules (RRDS) is a policy document that defines standard, legally approved retention periods and disposition instructions for official records regardless of storage media. In other words, the RRDS applies to official records, including paper records, electronic records, and microfilmed records.

The purpose of Records Retention and Disposition Schedules is to ensure that official records are:

- Maintained for as long as needed to satisfy legal, regulatory, and operational requirements.
- Disposed of in a systematic and controlled manner.
- Identified for preservation.

All records must be maintained for the correct prescribed length specified within approved RRDS unless needed as part of anticipated or ongoing litigation, audit, or legal regulations requiring an extended retention period. The University Records Retention Schedules are accessible on the USG's and the Office of Legal Affairs' website.

2.1 The organization of the Records Retention Schedules

Records Retention and Disposition Schedules list records and specify how long they must be kept. Records are arranged in categories according to their administrative function. For example, all financial, fiscal, or accounting records are grouped under "Finance." Many administrative units, offices, programs, or departments may create, use, and maintain these records. The category title does not imply that the records are the sole responsibility of a specific area.

Records Category: Group of similar or related record series arranged by category and related as the result of being created, received, or used in the same activity.

Record Series Title: A unique title for each record series is listed on the RRDS.

Record Series Number: A unique nine-digit identifier for each record series listed on the RRDS.

Description of Records Series: A brief description of the information or documents contained in the records series.

Retention Period: The minimum retention period for the records group.

2.2 Amending the Records Retention Schedules

The University's Records Retention Schedule is created by the Georgia Archives of the University System of Georgia and adopted by the University President. The retention guidelines specify how long records are kept. Records retention periods address the University's legal, regulatory, and operational requirements as determined through consultation and collaboration with the Chief Legal Officer and other knowledgeable and accountable personnel in appropriate university offices.

Amendments, as expected, will need to be made to the RRDS to comply with legal, regulatory, or operational requirements changes. The Records Management Officer will notify the Georgia Archives of amendments that should be made to the schedules. Also, the Georgia Archives and the USG will notify the Records Management Officer of any changes that affect the University's obligations regarding the retention of records.

Section 3 Implementing the Records Retention Schedules

Ensure you use the most recent version of the Records Retention and Disposition Schedules. Printing and filing of retention schedules for future reference will often result in the use of obsolete and incorrect information. The online version on the USG's website is the official, up-to-date retention schedules to use when preparing records for destruction. Classify your records, where possible, under an appropriate records series at the time of creation or filing.

Use the searchable databases to assist in locating the records series. When using the search function, refer to the schedule with the correct series number for the most accurate series description and retention information.

3.1 Records Destruction

The University manages several categories of records destruction:

- Disposal of unofficial records and non-records.
- Destruction of official records.

3.1.a Disposal of unofficial records and non-records

The Records Retention and Disposition Schedules identify official records regardless of storage media and establish their retention requirements. Employees create and maintain other unofficial records not governed by the RRDS and thus may be destroyed when the record is no longer needed for reference use. Unofficial records should not be maintained longer than the official record.

Unofficial or non-records include the following:

- Duplicates of official records are not required to be retained for business or legal purposes.
- Informational copies or duplicates of records captured in a recordkeeping system and maintained for reference purposes, such as copies of correspondence, memos, and reports.
- Duplicates of internal publications, such as brochures and other collateral material, are used for reference purposes.
- Documents that do not reach the status of a record because they do not provide evidence of a business action. For example, an employee creates a draft agreement that is not sent, thereby not executing a business action. This documentation is commonly referred to as "non-record" material and thus not identified in the Records Retention Schedule. Drafts or versions of documents, therefore, can be destroyed when the final record is captured in a recordkeeping system.
- External documents and publications, such as trade journals and catalogs, which are not supporting documentation of business activities, are also non-record material and may be destroyed when no longer referenced.

3.1.b Destruction of all other official records

The following procedures apply to official records stored by university offices. Official records that have met the RRDS requirements and are not subject to legal holds should be destroyed.

3.1.b.1 Certificate of Records Destruction

Once official records listed on the Records Retention and Disposition Schedules have satisfied their required retention period and are not subject to a legal hold, those records may be eligible for destruction.

Before destroying or disposing of official records, the Certificate of Records Destruction form must be completed and signed by the University Records Management Officer, the department supervisor, and the RML. This form documents proposed record destruction

and, ultimately, the date of their destruction. Once the department receives all approval signatures, the records listed on the certificate will be destroyed.

The Certificate of Records Destruction is available on the Records Information Management website.

If official records are not listed on the RRDS, contact the Records Management Officer before destroying the records.

3.1.b.2 Destruction Method

Records of a confidential or proprietary nature must be shredded, destroyed, purged, or deleted confidentially and securely. It is recommended that departments utilize the approved shredding and destruction services of the University for efficiency and security. Records that do not contain confidential or proprietary information may be disposed of using regularly established university practices for handling waste paper.

Electronic records or devices must be destroyed or deleted such that Personally Identifiable Information (PII) cannot be read or reconstructed.

It is imperative that all employees actively monitor their possession and use of non-official University records (i.e., duplicates or copies). When in doubt if records contain confidential or proprietary information, always err on the side of caution and have the records shredded, destroyed, purged, or deleted confidentially and securely.

3.2 Transferring Records to University Special Collections

When conducting business, the University creates and maintains many records. Most of them must be retained for a short time as defined in the Schedules, but some records must be kept longer because of their continued value to the University. These archival records are preserved because they:

- Enable better quality planning, decision-making, and action by providing continuity, access to past experiences, expertise, knowledge, and a historical perspective.
- Provide a source for understanding the history of the University of West Georgia.

The University Archivist will review the RRDS to identify records of continuing value and provide records transfer procedures to university offices. Records Management Liaisons who have questions about how to transfer documents to the University's Special Collections should contact the University Archivist directly. Records may be transferred to the University Special Collections once the originating department no longer needs them. Once Special Collections receive records, the records are then under their legal custody.

Section 4 Suspension of Retention Schedules

When legal action involving the University is commenced or reasonably anticipated, the University must preserve all documents and information that may be relevant. As such, as soon as the Chief Legal Officer (CLO) is aware of circumstances that give rise to the duty to preserve, a "Legal Hold" directive will be issued to key individuals who may retain records that fall within the scope of the Legal Hold.

The Chief Legal Officer is the only individual with the ultimate authority to issue or release a Legal Hold that suspends the retention requirements for records. However, the CLO may work with the Records Management Officer (RMO) to develop procedures for communicating with key individuals and RMLs regarding initiating and releasing Legal Holds. The RMO will maintain a listing that details the status and progress of Legal Holds.

Individuals notified of a Legal Hold may not transfer, dispose of, alter, or destroy any document or information that falls within the scope of the Legal Hold. Violation of the Legal Hold may subject the individual to disciplinary action, up to and including dismissal for employees, as well as a potential legal sanction by the applicable court or law enforcement agency.

Records under a Legal Hold
CANNOT BE DESTROYED.

ALL regularly scheduled destruction
MUST IMMEDIATELY be SUSPENDED
even when permitted by the
University's Records Retention
Schedule.

4.1 Initiation of Legal Holds

As soon as the University is aware of circumstances in which it is necessary to initiate a Legal Hold, the Chief Legal Officer or their designee will issue a hold directive to key individuals who may possess records that fall within the scope of the Legal Hold. This directive will describe, among other things, the subject matter and scope of the records to be preserved.

Additionally, the CLO will notify the RMO that a Legal Hold has been issued and communicate (a) the individuals and departments affected by the Legal Hold and (b) the subject matter and scope of the records to be preserved.

Records Management Officer, in consultation with Chief Legal Officer, will work with (a) individuals in possession of documents subject to the Legal Hold; (b) Records Management Liaisons, and (c) Information Technology Services (ITS) to coordinate the initial and ongoing implementation of the Legal Hold. This coordination may include but is not limited to assisting with locating and gathering records that fall within the subject matter and scope of the hold, communicating preservation instructions, training as needed, and monitoring ongoing compliance with the Legal Hold.

4.2 The Scope of Legal Holds

While all University records are potential sources subject to a Legal Hold, only those that fall within the scope of the Legal Hold may include but are not limited to:

- (a) Email messages and attachments: (these may be in mailboxes stored on network mail servers, individual archived messages [PST files], individual message files, or on mobile devices, or printed hard copies);
- (b) User-created files such as word processing documents, spreadsheets, and image files stored on the hard drives ("C Drives") of computers and workstations or network shared drives;
- (c) Hard copy files;
- (d) Database systems (e.g., PeopleSoft, Banner, ADP);
- (e) Other electronic or "hard copy" information held or stored in electronic or hardcopy format under the control of the University (these may include, for example, data stored on CD-ROM or DVD, thumb drives, removable hard drives, magnetic media, computers, internet servers, Google drives, etc.).

As indicated above, records subject to a Legal Hold may only be considered for destruction once the Legal Hold is removed and communicated by the Chief Legal Officer or their designee. The Records Management Officer shall monitor reports and listings of records to be considered for destruction to ensure that no records subject to a Legal Hold are disposed. UWG shall periodically review its processes and procedures related to Legal Hold to ensure they are useful.

4.3 The Release of Legal Holds

The Chief Legal Officer notifies the Records Management Officer when a Legal Hold is released. The RMO will then coordinate with (a) the individuals who possess documents subject to the Legal Hold; (b) the appropriate Records Management Liaisons; and (c) Information Technology Services (ITS) to communicate the processes for releasing the Legal Hold. This process will be documented to demonstrate approval from the Chief Legal Officer.

After a Legal Hold is lifted, Records Management Liaisons are responsible for resuming regularly scheduled destruction. According to the University's Records Retention and Disposition Schedules, records will be processed for disposal at the next destruction review date if the records retention period has ended.

Section 5 Records Confidentiality, Access, and Security

5.1 Records confidentiality and security

All employees must be aware of protecting the Privacy and security of University records and preventing unauthorized or inappropriate disclosure to third parties (i.e., persons inside and outside the University without a need to know). Also, all employees are responsible for compliance with all University policies and procedures regarding records information management. (See UWG [Policy #5003, Privacy](#) and associated procedure [Family Educational Rights and Privacy Act \(FERPA\)](#) and [Policy 1009, Legal and Regulatory Compliance](#) and associated procedure.)

5.2 Records security

The University's policies and procedures apply to the entire university community. These policies and procedures help:

- Ensure the security, availability, Privacy, and integrity of the University's information systems, networks, and data.
- Outline procedures for reporting breaches of information security.
- Ensure compliance with various federal and state regulations and other University information security-related policies and procedures.

Section 6 Training

The Records Management Officer will design and implement the University of West Georgia Records Information Management Program. Employees with records management roles and responsibilities will receive training. The content of the records management-training program will be reviewed periodically and updated to ensure consistency with current University records policies and procedures. The Office of Legal Affairs will also provide training for records information management throughout the year.

Section 7 Roles, Responsibilities, and Accountabilities

Data Governance

All USG institutions and organizations must have policies and procedures for the governance and management of data. Policies and procedures provide oversight and guidance of the various data governance and records management processes which inform the University System of Georgia (USG) business operations, including but not limited to: definitions, collections, usage, reporting, protection, and preservation. The appropriate management of data is the responsibility of all University employees but is of particular concern to the offices and/or positions responsible for the activities described below.

Policy originates from the Board of Regents (BOR) and is captured in the BOR Policy Manual. This policy, as well as procedures and guidelines from the USG Business Handbook and USG Information Technology Handbook, directs the governance and management of USG enterprise data. The University of West Georgia, as an individual USG institution, has developed additional procedures for the Institution's records management and data governance processes, provided these procedures do not conflict with the policies described by the Board of Regents.

For detailed definitions and responsibilities of Owners, Stewards, Trustees, and Users, refer to USG Business Procedures Manual Section 12.2 Governance Structure and USG Information Technology Handbook Section 1, Information Technology (IT) Governance.

7.1 Data Owner (University President)

Individual USG institutions are responsible for the data created, updated, deleted, collected, read, and reported by the Institution. As a chief executive officer, the president of the USG institution is identified as the data owner of institutional data and is responsible for identifying, appointing, and holding data trustees accountable.

7.2 Data Trustees

Data Trustees, appointed by the Data Owner, are executives of the Institution who have overall responsibility for data management and administration in their respective functional areas.

7.3 Data Stewards

Data Stewards, designated by Data Trustees, are offices/positions responsible for the data read, used, created, collected, reported, updated, or deleted, and the technology used to do so in their functional areas. Data stewards may report directly to a data trustee, recommend policies to the data trustees, and establish procedures and guidelines concerning the access to, completeness, accuracy, Privacy, and integrity of the data for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas. Depending on the size and complexity of a functional unit, it may be necessary and beneficial for a designated data steward to identify associated data stewards to manage and implement the stewardship process.

7.4 Chief Information Officer (CIO)/ Chief Information Security Officer (CISO)

The responsibilities of the CIO and CISO are to ensure that technical infrastructure is in place to support the data needs and assets, including availability, delivery, access, and security across their operational scope.

7.5 Data Users

Data Users are any UWG employee authorized by the appropriate institutional authority to access University data or data related to their respective institutions. This authorization should be for specific usages and purposes and designed solely for conducting institutional business.

7.6 Information System Owner

This individual, within the organization, should be the senior person responsible for the application or service and who ensures the use or service renders value to the organization. However, the designation is dependent upon the organizational structure.

Records Information Management

Employees must manage University Records in a trustworthy manner that ensures their authenticity and usefulness.

Departments and offices have the responsibility to ensure that their employees:

- Create records that adequately and accurately document core activities.
- Manage and store records to facilitate timely and accurate retrieval.
- Ensure records are stored in authorized, secure locations and stable environments.
- Allow only those with the proper authority to access records information systems.
- Know and carry out the proper disposition of their records.
- Know and comply with University RIM policies and procedures.
- Know and comply with external laws, regulations, standards, and professional ethics that affect records management.

In addition, to be above, it shall be the responsibility of the department to ensure the following:

- Review the types of University records in its possession and determine appropriate formats to ensure usability, integrity, and accessibility for as long as the records are needed.
- Adopt and implement written procedures specific to all records managed by the department or office.
- Assign a Records Management Liaison for all departments.
- Train and educate staff concerning this Policy and any departmental or office procedures for handling records.
- Consult with the University Archivist regarding the appropriate disposition of records that may be of permanent, historical, or legal value to the University. If determined that some department/office records should be transferred to University Special Collections, each department or office is responsible for arranging the complete and timely transfer.
- Ensure that access to records and systems containing Personally Identifiable Information (PII) is restricted from public access or disclosure. Long-term restrictions on access to selected Archival Records must be noted at the time of their transfer to the University's Special Collections.
- Destroy Inactive Records that have met their authorized retention period per the University Records Retention and Disposition Schedules (RRDS).
- Destroy Duplicate Records (including duplicate electronic records) immediately upon determining that such documents are no longer necessary to fulfill the mission of the department or office.

Employees are urged to visit the Records Information Management website <https://www.westga.edu/administration/president/legal/rim/index.php> to keep up to date as changes to procedures and retention schedules occur.

7.7 Information Technology Services (ITS)

Information Technology Services is responsible for providing appropriate storage and media in addition to procedures and systems to protect records on ITS-managed electronic media in conjunction with the Records Retention and Disposition Schedules and/or Legal Hold Orders. It may include purchasing, designing, modifying, or redesigning information systems, business applications, and communication systems to create and capture official university records.

7.8 Chief Legal Officer

The Chief Data Officer, appointed by the Data Owner, is responsible for overseeing the University-wide implementation of policy, including creating, implementing, and monitoring department/office-specific policies and procedures that incorporate, at a minimum, the elements outlined in Policy 1008 Records Information Management.

Chief Legal Officer or their designee is responsible for:

- Authorizing suspension of the routine destruction of records.
- Authorizing the release of legal holds.
- Notifying University Records Management Officer of significant changes in the law that necessitate a review of the records information management policies and procedures.

7.9 Office of Legal Affairs (OLA)

The Office of Legal Affairs promotes awareness and understanding of RIM policies and procedures by providing training and services to the University community.

7.10 University Records Management Officer (RMO)

The University Records Management Officer, designated by the Chief Legal Officer, oversees the university-wide implementation of the RIM Program and is responsible for:

- Managing and implementing a records information management program for the university.
- Issuing official updates to the University's record retention schedules.
- Establishing and implementing standards for University's records and recordkeeping practices.
- Issuing and implementing records information management procedures and guidelines.
- Educating and training employees on records information management policies and procedures.
- Working with Records Management Liaisons and executive management to ensure the effective management of the program.
- Identifying budget and staff requirements for the RIM program.
- Working with the University Archivist to identify records of continuing value.

7.11 Records Management Liaisons (RML)

Records Management Liaisons are critical to the successful implementation of the records information management program, whose activities include:

- Serving as a liaison between their department and the University RMO.
- Attending and participating in records information management training and exercises.
- Implementing RIM policies and procedures within their office.
- Coordinating destruction of official records according to the Records Retention and Disposition Schedules (RRDS).
- Classifying and indexing official records before transferring them to off-site storage.
- Submitting recommendations for the RRRDS.
- Training staff and faculty in their area to perform specific tasks associated with RIM.

- Promoting the RIM program and use of the RRDS.
- Coordinating and encouraging participation in annual file destruction.
- Coordinating the gathering and protection of records in response to legal requirements.

7.12 Records Information Advisory Group

The Records Information Advisory Group (RIAG) comprises the Chief Legal Officer, University Archivist, Information Security Officer, and the University Records Management Officer, with additional staff added as needed. At their discretion, the RMO may convene the Records Information Advisory Group to develop procedures for implementing the RIM policy.

This group is responsible for:

- Approving amendments to the Records Information Management Policy.
- Reviewing RIM procedures as needed to address changes in recordkeeping practices.
- Ensuring that the RIM Program is maintained and updated.
- Guiding records management initiatives and activities.

7.13 Third Parties

Third Parties who manage University Records are responsible for compliance with the University recordkeeping requirements and making University records available upon request by authorized personnel. The Data Owner and trustees are accountable for ensuring that third parties on their behalf comply with all applicable recordkeeping requirements and standards.

Section 8 Records Policies, Procedures, and Practices

O.C.G.A. § 50-18-90 through § 50-18-121 "the Georgia Records Act" provides guidelines for the establishment of retention schedules and the duties of agencies with regards to records management and access to records.

University Policy establishes a Records Information Management (RIM) program to provide structure, responsibilities, and procedures by applicable federal and state laws and regulations. The policy adopts the USG Records Retention and Disposition Schedules for the retention of official university records. The Chief Legal Officer or designee is authorized to establish procedures for compliance with this Policy.

The designated Records Management Officer (RMO) is authorized to issue procedures and guidelines necessary to promote the proper management of University records to help ensure compliance with applicable records laws, regulations, and best practices; and to improve efficient university recordkeeping.

Records Information Management Program Maintenance

Updates to the RIM program and policy will occur to account for changes in legal, regulatory, or operational requirements. The following sections of the USG Policy Manual and Information Technology Handbook should be reviewed annually to align the RIM program to the University System of Georgia policies.

USG Business Procedures Manual

https://www.usg.edu/business_procedures_manual/print/section12

Section 12.0 Data Governance and Management

Sections 12.1 – 12.2.1 of the USG Business Procedures Manual should be reviewed annually.

USG Information Technology Handbook

https://www.usg.edu/assets/information_technology_services/documents/IT_Handbook.pdf

Section 1 Information Technology (IT) Governance

Section 3: Information Technology Management

3.1: Information System User Account Management

Records Management Liaisons should notify the Records Management Officer if changes are needed. The RMO notifies the Records Advisory Group of any proposed recommendations to the schedules and/or procedures.

The Records Advisory Group may periodically review proposed changes to the Records Retention and Disposition Schedules and/or have the retention periods examined through legal and regulatory research deemed necessary by the committee.

Appendix A - Vocabulary

For a complete listing, refer to the USG's Glossary of Terms
https://www.usg.edu/records_management/glossary/

Access

The right opportunity means finding, using, or retrieving information.

Active-Record

A record frequently referred to or needed to support the current business activity of a unit.

Administrative Records

Records that concern information on the routine operation and management of any office.

Administrative Value

Value of a record based on a continuing need for it or its usefulness for conducting business.

Archival Records

Records appraised to have archival or continuing value; storage for historical documents and artifacts; the program responsible for selecting, acquiring, and preserving archives, making them available, and approving their destruction. (*See Permanent Record*)

Archives

An area used to permanently store valuable documents for the benefit of scholars and future generations.

Archivist

Individuals responsible for collecting and managing records of enduring value to protect their authenticity and context.

BackFile Conversion

The process of scanning in, indexing, and storing a large backlog of documents on an imaging system.

Backup

To create a copy of records as a safeguard against the loss or damage of the original material

Calendar Year (CY)

Twelve months beginning January 1 and ending December 31.

Certificate of Records Destruction

Form for recording destruction of official University records that have met retention requirements listed in the Records Retention Schedule.

Chronological Files

Files arranged in date order.

Chronological Filing

Files arranged in date sequence.

Classification

Assigning a file series (or class) to a document.

Closed File

A file folder in which documents should not be added.

Confidential Records

A record to which public access is or may be restricted or denied under the Georgia Open Records Act, O.C.G.A §50-18-70, or other federal or state law.

Cubic Foot (c.f.)

The standard measure of volume equaling 15" L x 12" W x 10" H. To determine the cubic footage

$$\frac{L'' \times W'' \times H''}{1728}$$

Current files area

The area in which frequently used records is maintained.

Cut Off Event

A point in time when a record series can be broken into a regular segment and its disposition applied to that segment.

Delete

Electronic removal from the memory of a file's index, not the file itself. Deleted records may remain on storage media in whole or in part until overwritten and may be restored with complete accuracy.

Destruction

The process of eliminating or deleting records, beyond any possible reconstruction.

Destruction Date

The date marks the end of the legally required retention period for non-permanent records when records are destroyed unless the records are involved with or relevant to an audit, litigation, or continuing administrative action.

Digital Image

Image composed of discrete pixels set in rows and columns to form a composite eye-readable format. Appropriate techniques and quality control processes must be used, and duplication is a regular business function/activity practice.

Digitized Records

Records created or converted into a digital image.

Discovery

The legal process that compels a party in a lawsuit to disclose information or records relevant to a court case.

Disposition

Process for removing inactive records from active storage areas for off-site records storage, management in the archives, or destruction.

Document (noun)

Recorded information or object that is treated as a unit.

Duplicate File

A photocopy of the official record created for easy reference, not located in the Office of Record.

Electronic Records, Electronic Data, Information and/or Record

Information recorded in a machine-readable format (e.g., information that only a computer/machine can process and which, without a computer/machine, would not be understandable to people). These include but are not limited to electronic digital interchange, email, digital/text voice messages, instant messages, and text messages.

Email

An Internet protocol that allows computer users to exchange messages and information in real-time with other users, locally and across networks. Email is not a particular document type but a delivery method for many document types. While some email messages may be official records, others are not.

Emergency (Disaster) Plan

Policies, procedures, and information to direct necessary actions needed to recover from and lessen the impact of an unexpected interruption of business, whether natural or human-made.

Essential (or Vital) Records

Records immediately necessary to begin recovery of business after a disaster or essential to protecting the rights and interests of the organization, its employees, and the citizens of the commonwealth.

Fiscal Value

Value of a record based on continuing usefulness for verifying financial information necessary for conducting business.

File Series

A set of documents all having the same subject. For example, invoices, purchase orders, resumes, job descriptions, and meeting minutes are different documents.

Fiscal Year (FY)

Twelve-month period on which a budget is designed usually does not coincide with a calendar year. UWG's fiscal year begins July 1st and ends June 30th.

Folder List

List prepared by the creating office detailing the contents contained in one or more boxes, file drawers, or another storage container.

Format

The physical form/media in which material appears — books, slides, photographs, film, recordings, etc.

Historical Value

Value of a record based on its uniqueness, age, or exceptional significance.

Imaging

The process of copying documents by reproducing their appearance through photography, micrographics, or scanning.

Inactive Records

Records related to final, closed, completed, or concluded activities. Records become inactive when no longer routinely referenced but must be retained to fulfill legal, regulatory, operational, or other retention requirements. Inactive records should be stored securely until the end of the designated retention period. Unless these records are defined as permanent, they should be destroyed after the specified retention period has elapsed.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner

An individual within the organization responsible for the application or service and who ensures the use or service renders value to the organization.

Input

In electronic records, data is entered into a computer for processing.

Input Records

Non-electronic documents used to create, update, or modify records in an electronic medium, or electronic records containing data used to update a separate computer file, sometimes called source records or source documents.

Legal Hold

The procedure used to cease the destruction of specific groups of records temporarily, even if they are eligible for destruction.

Legal Value

The value of a record is based on its ability to document and protect the rights of citizens, provide defense in litigation, or demonstrate compliance with the law.

Life Cycle of Records

Distinct phases of a record's existence, from creation to final disposition.

Linear Feet

Linear feet (often called Lineal feet) are the same as regular feet. No conversion is necessary. If something is six linear feet tall, it is 6 feet tall.

Metadata

Data describing the context, content, and structure of records and their management through time.

Non-Record Material

Material or documents excluded from the legal definition of a (public) record, such as copies of documents kept only for the convenience of reference, extra copies of printed records or publications, and materials intended solely for reference or exhibition. Non-record documentation does not appear on a records retention schedule and may be destroyed without authorization. Non-record copies of documents are kept solely for ease of access and reference.

Off-site Storage

An off-site storage facility is a place of business where records are stored for protection other than usual.

Official Records

The complete (final), authoritative version, retained and required for business or legal reasons. Official records provide evidence of the University's organization, business functions, policies, decisions, procedures, operations, and internal or external transactions and reflect the University's intent to preserve such information. Official records must be retained for the entire retention period. Records are considered official when they are in their final form and held by the designated Office of Record.

Office of Record

The unit, department, or division responsible for the retention and timely destruction of official University records and assigned to the unit's administrator or a designee.

Output

Information transmitted from internal to external units of a computer or an outside medium.

Output Records

Computer-generated information placed on an outside medium, such as paper, microform, or an electronic storage medium.

Overwrite

To write new electronic data on top of existing electronic data and thus erase the previously existing data.

Permanent Record (or Archival Record)

Records appraised as having sufficient historical or other value to the University to warrant continued preservation beyond the retention period for administrative, legal, or fiscal purposes. (*see Archival Record*)

Personally Identifiable Information (PII)

Information used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information linked or linkable to a specific individual. PII is not anchored to any single category of information or technology. Instead, it requires a case-by-case assessment of the particular risk that an individual can be identified. When performing a risk assessment, an agency must recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, combined with other available information, could be used to identify an individual. Examples of PII include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

Personal Papers or Files

An individual's private papers related to their personal affairs and excludes agency business. Personal papers must be designated as such and kept separate from the agency's records.

Preservation

The act of stabilizing storage environments and records to ensure the continued existence, accessibility, and authenticity of documents over time.

Privacy-Protected Record

A record containing personally identifying information (PII) safeguarded from disclosure.

Public Record

A record open to public inspection by law or custom. According to the Open Records Act, (O.C.G.A. 50-18-70), (public) records are "all documents, papers, letters, maps, books, tapes, photographs, computer-based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency."

Record

Information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or the transaction of business.

Records Center

Storage space or facility for the high-density and low-cost storage and maintenance of semi-active or inactive records pending their final disposition.

Records Management Officer

A University employee appointed to direct and oversee the University Records Information Management Program established under Georgia Records Act, O.C.G.A. §50-18-90.

Records Inventory

The process of surveying records to determine the size, scope, and intricacy of the department/agency's records. It should include the record series, inclusive dates, types of records, quantity, arrangement, and description.

Records Management

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records Information Management (RIM) Program

A comprehensive plan created to systematically control the creation, maintenance, use, and disposition of physical and electronic records. The RIM Program is the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in records creation, maintenance, use, and disposition to achieve adequate and proper documentation of the policies, processes, and transactions at the University.

Records Inventory

A survey of records to determine the size, scope, and intricacy of the department/agency's records. It should include the record series, inclusive dates, types of records, quantity, arrangement, and description.

Records Management Liaison (Departmental)

University staff designated by the department or unit head to coordinate records management activities for the department.

Records Series

A group of identical or related records utilized, filed and disposed of similarly. (Human Resources & Student records are examples of Record Series, while College Department Student Files and Veterans Records are types of records that fall under the Student Records Series. Each record type would have a separate Retention schedule.)

Records Storage Box

Standardized storage container designed to house either letter- or legal-size files on a standard shelving unit. The carton is approximately one cubic foot in volume or 15" x 12" x 10" in size.

Reformat

A record copied/recreated in a different format or medium from the original, especially for preservation or access needs.

Removable Media

Any portable computer storage device that can be easily removed from a computer and stored or transported separately, including, but not limited to, CDs, DVDs, flash drives, floppy disks, DAT tapes, cartridges, and Zip disks.

Records Retention Schedule

A document that describes the University's records, establishes a length of time records shall be retained, and provides instructions for the disposition of records throughout their life cycle to assure records are retained for as long as necessary based on their operational, financial, legal, and continuing value.

Retention Period

The minimum length of time records must be kept for legal, regulatory, operational, or other purposes.

Security

Measures to protect materials from unauthorized access, change, destruction, or other threats.

Sensitive Data

Information inappropriately disclosed that might cause harm to an individual or Institution includes academic (FERPA), medical (HIPAA), and identity numbers.

Scanner

A device that optically scans a human-readable image and converts the image to machine-readable code with applicable software.

Schedules Records

Records for which there is an official records retention schedule.

Shredding

Means of destroying paper records by mechanical cutting.

Transfer

The process of moving records from one location to another, changing custody, ownership, and/or responsibility of records.

Transitory Records

Routine correspondence with short-term records value destroyed after the action covered by this correspondence is completed.

Transmittal Sheets

Used by agencies in transferring records to University Special Collections, Off-site storage, or State Records Center, which lists box contents along with other statistical data.

University Special Collections

A repository for particular, permanent, inactive records created at the University of West Georgia. University Special Collections are housed in the Ingram Library. The University Special Collections documents the administrative, research, student, and staff activities on campus from the University's establishment to the present. The Library's holdings include correspondence, publications, audiovisual materials, and photographs, among many other types.

Unofficial Records

Records that are not required to be retained for business or legal reasons. These may include duplicates or "convenience" copies of official records that have not been annotated and may be destroyed when no longer referenced.

Until Obsolete

Retention period assigned to records that become valueless on a non-routine basis.

Until Superseded

Retention period assigned to records that are routinely updated or revised and where the previous version has no continuing value.

Working Copies/Drafts (Reference Only Copies)

Documents with short-term or transitory use and used as reference only. May include rough notes, calculations, or drafts used to prepare or analyze other documents. Working copies are documents that have no administrative, operational, financial, legal, or historical value. An example of a "draft" is a proposed contract before a final signature; the final contract is the official record; the preliminary revisions are drafts. An example of a "working file" is the communication between parties discussing the various terms that may be included in a proposed contract. In some specific cases, such as audit working papers or calculations that support project reports, working (active) files may be considered an integral part of the official University Records.