

# Records & Information Management

# Handbook

## Table of Contents

Objectives .....	1
What Is a Record? .....	1
What Is Not a Record? .....	1
Records and Information Management ...	1
Public Records .....	2
Value of MCCCDC Records .....	2
Managing Records .....	2
Custodian of Record .....	2
Retention Schedules .....	3
Disposition of Records .....	3
Creating a New Retention Schedule .....	3
Considerations for E-Documents .....	3
Electronic Imaging of Paper .....	4
Data Management .....	4
Access, Use and Protection of Data .....	4
Authorized Access .....	4
Acceptable Use .....	4
Reasonable Protection .....	4
Custodian of Record Accountability .....	4
Metadata .....	5
Some Helpful Definitions .....	6
<b>Appendices</b>	
Frequently Asked Questions .....	8
Lifecycle of Records .....	10
Is It A Record? .....	11
MCCCDC Document Destruction Services ...	12
Records Inventory Worksheet .....	13
Records Retention Schedule .....	14
Certificate of Records Destruction .....	16
Imaging Requests .....	17-21
Management & Protection of Data .....	22
Principles of Acceptable Use .....	24
Reasonable Protection .....	25
Student Records .....	26
Electronic Communications and Records Requests .....	28

## Records and Information Management (RIM) for MCCCDC

### Objectives

This handbook serves as a resource to help Maricopa Community College employees (faculty, staff and administrators) to appropriately manage records and information. It will also provide guidance on records and information management which includes storage, archiving, disposition and reporting to state agencies. As a political subdivision of the State of Arizona, many of the records of the Maricopa Community Colleges are considered public records (with some restrictions) and subject to review by any member of the communities we serve. To this end, records and information need to be organized and easily retrieved if a member of the public were to request to review them.

This handbook provides a brief look at what records, records management, information, and information management are, how they relate to the Maricopa County Community College District (MCCCDC), the types of records and information the MCCCDC has and how to manage them and how to create records and information inventories for specific areas within the District as needed.

For the purposes of this handbook, “area” is used for simplification. “Area” can be substituted with: department, division, constituency group, or functional location (i.e., admissions and records/student enrollment services, human resources, a College, District Office, etc.) to describe a noted records custodian.

### What Is a Record?

As defined by state statute ARS §41-1350, **records** are: *all books, papers, maps, photographs or other documentary material, regardless of physical form or characteristics... made or received... in connection with the*

*transaction of public business... Records may include computer-based records, voicemail, text messages, email, photographs, motion pictures, video and audio recordings, charts, maps, drawings, plans, micrographics and more.* The format that information exists in is not as relevant as the actual **value** that the item has to the Maricopa Community Colleges.

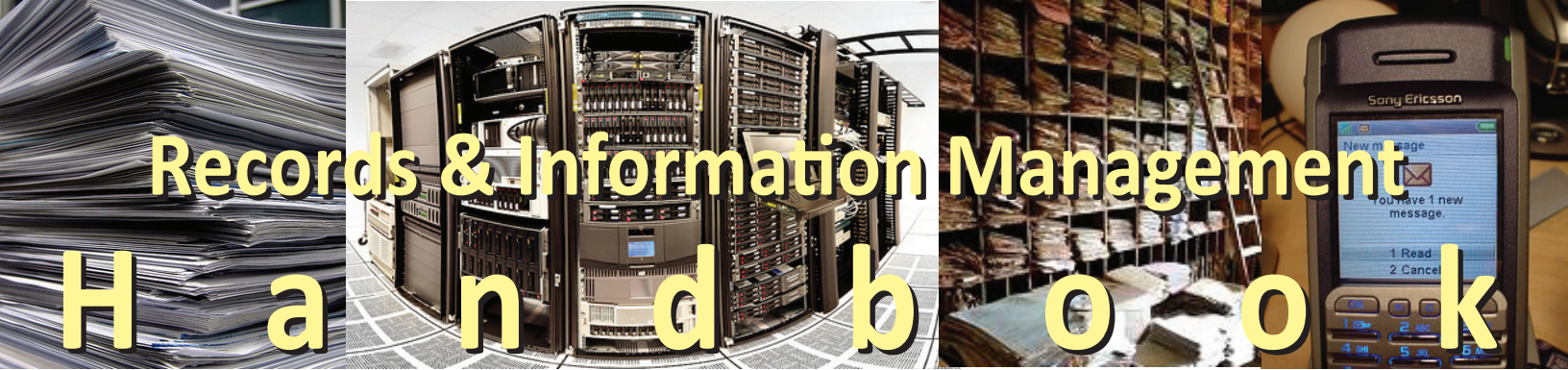
### What is Not a Record?

ARS §41-1350 states: *...material made or acquired solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference and stocks of publications or documents intended for sale or distribution are not included within the definition of records.*

### Records and Information Management

**Record management** is the maintenance and disposition of a record throughout its lifecycle. **Data** are institutional assets used to support instruction, student services and administrative functions. According to ARMA International ([www.arma.org](http://www.arma.org)), **information** is data that has been given value through analysis, interpretation or compilation in a meaningful form. Thus, **information management** is the practice of analyzing information as a resource of the organization—how that information will be acquired, recorded, organized, stored, retrieved and shared; information management helps to support the effective use of information within the organization.

For the purposes of clarification, in this handbook, we will use the terms “documents” and “data” to refer to work resources that have not been assessed a value and “records” and “information” as work resources that have. In most instances, “documents” will refer to paper-based assets and



# Records & Information Management

# Handbook

“data” and “information” will refer to electronic assets. Regardless, “record” is the universal term for a work asset that has been assigned a value by the organization, regardless of form.

**Retention** is the maintenance of records and information for further use (which includes security for confidential information) while **disposition** is the destruction of records and information with lawful authority based on an approved retention and disposition schedule by the Arizona State Library, Archives and Public Records. Destroying records without lawful authority is a class 4 felony (ARS §38-421), as is destroying records while a legal investigation is in action or pending (this is called **spoliation**). This would also include destroying records once notice is given that a public records request has been received.

Prior to release, all information in the records must be reviewed and items not subject to release need to be redacted (i.e., attorney-client privilege, personal information, federally protected information, etc.)

**Redacting** means to obscure or black out information that should not be disclosed. Copies should be redacted, not originals!

## Public Records

*All records made or received by public officials or employees of the state in the course of their public duties are the property of the state (ARS §41-1347(A)). Public records shall be open to inspection by any person at all times during office hours (ARS §39-121). All public bodies shall maintain all records...reasonably necessary or appropriate to maintain an accurate knowledge of their official activities and of any of their activities which are supported by monies from the state or any political subdivision of the state (ARS §39-121.01(B)).*

The MCCC is a political subdivision of the state, so many records created by the MCCC are considered public records. If a public records request is made, MCCC has the responsibility to disclose what’s requested. However, confidential

information is protected from release (except during a legal discovery process). Denying access to public records may occur if:

- the information is statutorily confidential or privileged (FERPA, HIPAA);
- the information falls within an individual’s right to privacy (personal address/phone, social security number);
- it is not in the best interest of the MCCC to release it (to do so would seriously impair performance of duties); or
- the records are sealed by Court Order.

## Value of MCCC Records

Documents and data are categorized according to their **value** to the MCCC in one of five categories:

- **Administrative:** Records have administrative value if they are needed to conduct an office’s daily business (i.e., procedures manuals, retention schedules, memos and reports).
- **Fiscal:** Records have fiscal value if they are needed to document the audit trail of monies (i.e., budget records and expenditure reports, wage and salary, benefits or business forms—petty cash vouchers, book vouchers, travel requests, expense claim forms, invoices, etc.)
- **Legal:** Records have legal value if they meet specific legal requirements to keep them for a given period of time which are found in the Arizona Revised Statutes (ARS), United States Code (USC) and Code of Federal Regulations (CFR). This includes any agreements between MCCC and another entity or that MCCC uses to regulate itself by aligning with State/Federal laws (i.e., contracts and agreements, administrative regulations and Governing Board policies).
- **Historical:** Records have historical value if they detail the conception, creation, operation and evolution of MCCC and its community partnerships (i.e., Governing Board minutes, chancellor or president papers, college history and photos, plans or architectural renderings).
- **Academic / Instructional:** Records that are used in the process of instruction (i.e.,

course syllabi, instructional materials and student work—papers, exams, projects, portfolios, art work, performance pieces, etc.). Although student work is not subject to release it must be protected as confidential information.

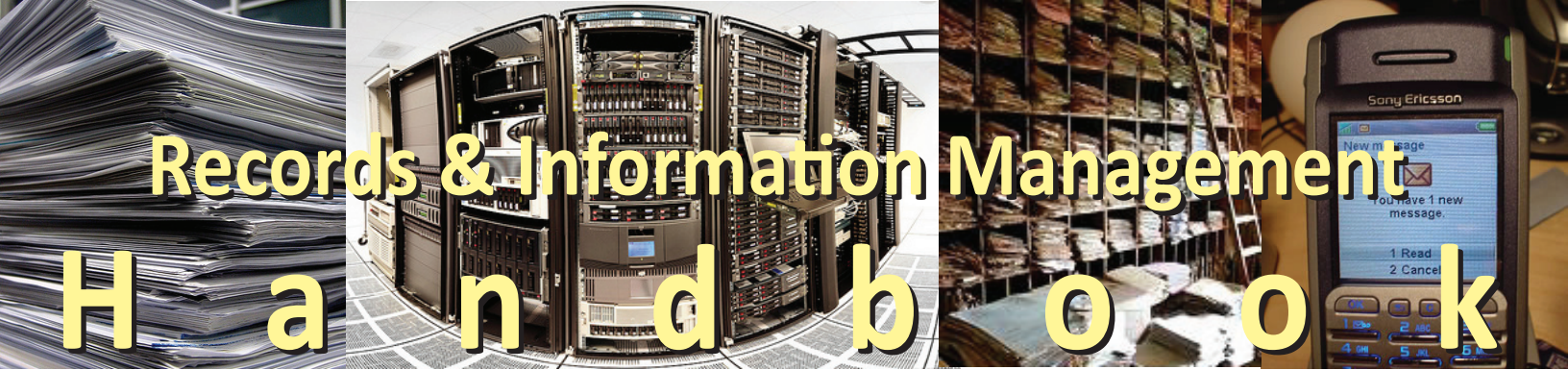
## Managing Records

Who is responsible for managing records and information for the MCCC? The simple answer is ... everyone. Faculty, staff and administrators (whether full-time, part-time, OSO, OYO, temporary or adjunct) are responsible for the documents and data they create in the course of daily operations. All Maricopans are responsible for knowing about records and information management and records release. The Office of Public Stewardship provides training and guidance on records and information management.

## Custodian of Record

The custodian of record is considered the party or area at a College, Center or at the District Office designated as being responsible for the maintenance, retention/archiving and disposition of specific records. The custodian of record will also oversee the review of records prior to release as well as the reproduction of records when requests for copies are made.

Who the custodian of record is will depend on who created the record, its purpose and who has jurisdiction over the final document. Creating a **Records Inventory** (see appendices, p. 11) will help determine which records an area is responsible for. Additionally, it is extremely important to understand the process a document may go through to determine who holds the official record. In most cases, the creator of the document is considered the custodian of record. However, in instances where the document needs to be signed or in which the “original” is considered the official version, that document, wherever it ends up, is the record.



# Records & Information Management

# Handbook

## Retention Schedules

A retention and disposition schedule approved by the Arizona State Library, Archives and Public Records for Arizona Community Colleges and Districts can be found online at [www.lib.az.us](http://www.lib.az.us). In the event documents in an area are not listed as part of the schedule, a new schedule can be created by working directly with the District's Office of Public Stewardship.

## Disposition of Records

Before records can be disposed of, check to see if there is a pending or imminent litigation, audit or government investigation under way. This information can be requested from the College president's office or Legal Services at the District Office. Ultimately, if there is any question about a hold on records, do not destroy anything even if the schedule says it is time.

If there is no legal action, audit or investigation pending, records may be disposed of in the following manner:

- non-confidential records may be recycled or thrown away;
- confidential records must be shredded or burned in a manner that ensures continued confidentiality;
- non-record copies should be destroyed at the same time and in the same manner; and
- a **Certificate of Records Destruction** (see appendices, p. 15) should be prepared and sent to the Arizona State Library, Archive and Public Records at the same time the records are disposed of.

In the event records must be held due to legal action, audit or investigation, the custodian of record should not destroy anything until the legal action, audit or investigation has been released or completed. Records may be boxed and marked for destruction at a later date, but they must remain available and accessible.

## Creating a New Retention Schedule

If the records created by an area do not fall within the categories already defined in the

retention schedule for Arizona Community Colleges and Districts, a new schedule can be created specifically for those records. The new schedule should be created with the help of the District's Office of Public Stewardship. To begin, it would be helpful to create a **Records Inventory** (see appendices, p. 13) first. Additional consideration may need to be given to the format of the documents since it has direct bearing on how they will be stored.

### 1. Determine the scope of work

- What does the area do?
- What documents show this?
- What is their value—administrative, fiscal, legal, historical or instructional/academic?
- How long should they be retained?  
Consider other factors that dictate the length of time records need to be kept (i.e., federal regulation, state statute, etc.)
- In what manner should they be retained and where?

### 2. Determine the custodian of record

- Who created it? Why?
- Where does it "go"?
- Where does it "end up"? Why?
- Who needs access and how quickly?
- How many copies exist? Who has them?

### 3. Determine the format of the document

- Was it created electronically and then printed for distribution?
- Was it created and subsequently shared electronically only?

### 4. Determine where the records are or will be housed

- Will it be stored at an individual's work station or in a central file?
- Will it be housed off-site (in another department or at a central location)?
- Is it saved on a local drive, external drive or a college/District server?
- If it's on an MCCCDC-maintained server, what is the process for backing-up the data and how often?
- Was a paper document scanned? By what agency? Where did the paper go once scanned?

## Considerations for Electronic Documents

Again, documents in electronic format (data) are considered records as long as their content has value to the Maricopa Community Colleges. They are subject to the same retention schedule as if they were on paper.

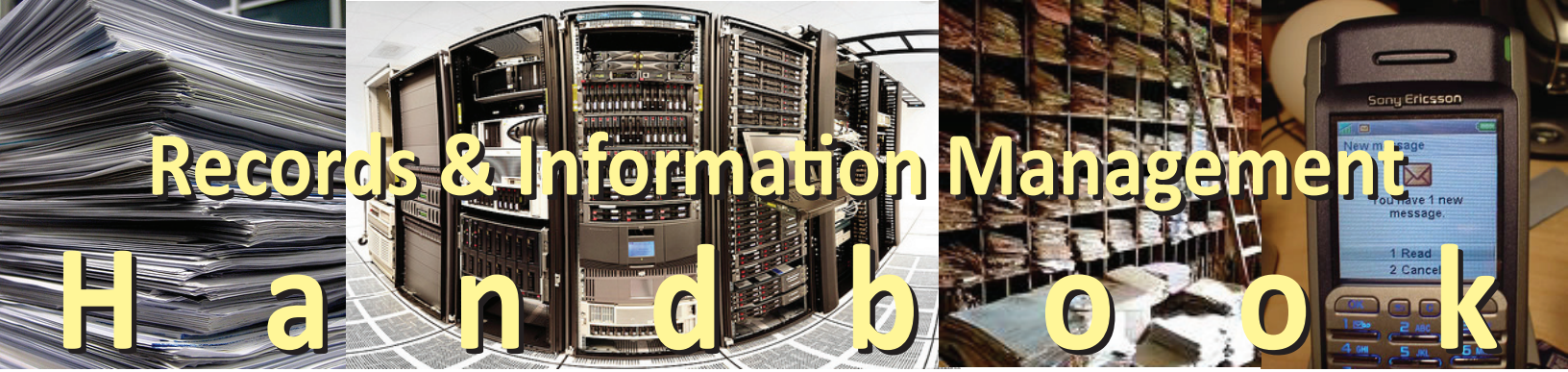
It is up to the custodian of record to ensure electronic records are maintained according to the approved retention schedule. It is generally not the responsibility of the department who maintains the area's computers or servers to ensure electronic records maintenance. The custodian of record should work with their Information Technology (IT) department to develop a suitable back-up plan or get recommendations for storage options for electronic records.

A **backup** is a copy of information created as a precaution in case the original is lost or stolen. **Archives** are those records in any medium that, because of their enduring historical or legal value, are retained permanently. **NOTE:** for electronic records, archive also describes a systematic way to organize and maintain e-records for the duration of their life cycle (a much more comprehensive plan than periodic 'backups').

**E-discovery** (as defined by ARMA International) are searches conducted in response to litigation, regulatory inquiries or investigations, and the objective is to search, retrieve and analyze ALL relevant documents an organization possesses. E-discovery can take up gigabytes of space, hundreds of hours of analysis and cost huge sums of money. Especially if e-docs are not archived and managed effectively.

## Electronic Imaging of Paper Records

Not all documents are suitable for scanning and electronic storage. Although some historical data lends itself to microfilm storage, originals still need to be preserved in their original form. The Arizona State Library, Archives and Public Records has created



# Records & Information Management

# H a n d b o o k

several criteria for imaging requests. For those documents which are suitable for scanning, there are five categories to consider. Imaging may be outsourced, but the custodian of record needs to ensure that the vendor can comply with the standards outlined in the requests (see appendices, pgs. 17-21):

- **Imaging Request for Minutes**  
Source Docs Not Destroyed
- **Imaging Request for Microfilm**  
Permanent Records
- **Imaging Request – Source Docs Not Destroyed** (<10 years)
- **Imaging Request – Source Docs Destroyed** (<10 years)
- **Imaging Request** (10+ years)

## Data Management

Following are MCCCDC best practices provided by the District's Information Technology department for data security, acceptable use and access management. (**Source Document:** [www.maricopa.edu/its/Process%20-%20DI%20Data%20Access%20Main%20Description.pdf](http://www.maricopa.edu/its/Process%20-%20DI%20Data%20Access%20Main%20Description.pdf))

## Access, Use and Protection of Data

Maricopa County Community College District (MCCCDC) recognizes its affirmative and continuing need to protect confidential employee and student data and to maintain the confidentiality of that data.

The MCCCDC Data Access and Appropriate Use Best Practice establishes appropriate and reasonable administrative, technical and physical safeguards designed to:

- ensure the security and protection of confidential information in its custody, whether in electronic, paper or other forms;
- protect against any anticipated threats or hazards to the security or integrity of such confidential information; and
- protect against unauthorized access to, or use of, such confidential information.
- define standards for obtaining access to data
- define limitations of access and appropriate use of data

**Data** are institutional assets used to support instruction, student services and administrative functions. While access and use of data is essential to accomplishing the MCCCDC's institutional mission, it requires the observance of critical standards to safeguard individuals' rights that are protected by state and federal laws or MCCCDC regulations. Therefore, MCCCDC has established a policy consistent with applicable laws regarding access, use and protection of data. The Chancellor shall establish through Administrative Regulation operational standards and practices regarding access, use and protection of data.

## Authorized Access

MCCCDC's intent is to make data as easily accessible as possible for the faculty, staff and administration to accomplish tasks related to their role and responsibilities. Access includes, but is not limited to, varied types of medium such as paper records, printed reports, computer screens, computer systems, electronic storage and network transmission. Please refer to **Custodian of Record Accountability and Management and Protection of Data** (see appendices, pg. 22) for more information.

## Acceptable Use

All employees and agents of MCCCDC and anyone working on behalf of MCCCDC are charged with the appropriate use of data. Use of data for personal gain without public benefit, for personal business or to commit fraud is prohibited. All individuals defined in the scope of this policy are prohibited from negligent or deliberate acts that could result in unauthorized disclosure of data. Please refer to **Principles of Acceptable Use** (see appendices, pg. 24) for more information.

## Reasonable Protection

All employees and agents of MCCCDC and anyone working on behalf of MCCCDC are charged with the protection of MCCCDC data. Under existing federal and state

legislation institutions of higher education are responsible for the confidentiality and integrity of data within their institution. These laws and regulations include but are not limited to:

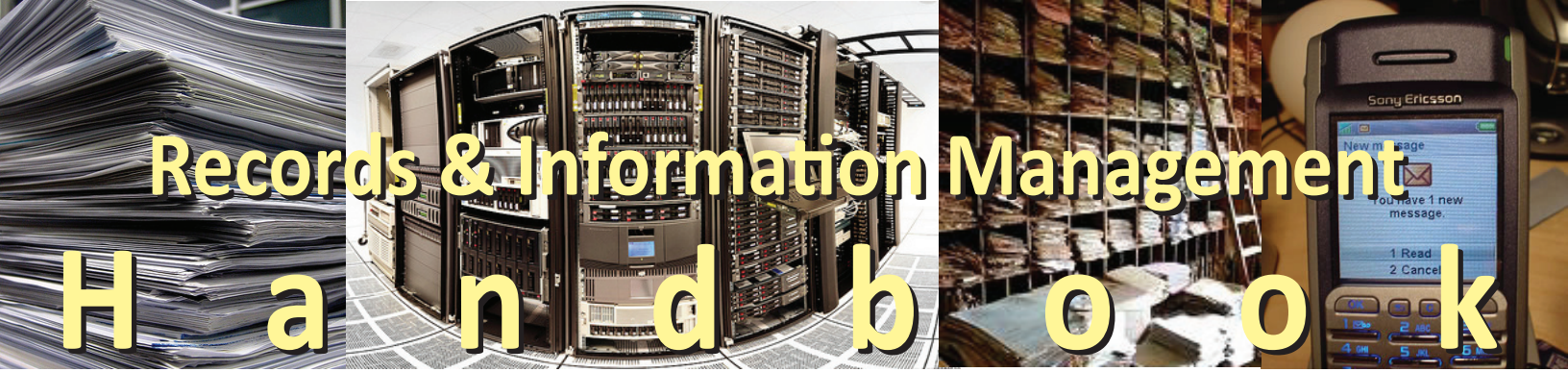
- The Family Educational Rights and Privacy Act (FERPA) – protection of student records
- Gramm-Leach-Bliley Act (GLBA) – protection of financial records
- Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002
- The Health Insurance Portability and Accountability Act – (HIPAA) – protection of health care records
- ARS §15-141. Educational Records; Injunction; Special Action

Please refer to **Reasonable Protection** (see appendices, pg. 25) for more information.

## Custodian of Record Accountability

Designated custodian of records should ensure that employees have access to District and/or College information systems and records as needed to perform their jobs or to achieve the lawful stated aims of a division executive. Custodians of Records should be familiar with the institutional ramifications of data access, security, quality and analysis, and should be cognizant of the state and federal regulatory mandates applicable to the category of data for which they are responsible. Therefore, custodians of records are charged with the following data administration responsibilities:

- Have designated duties for collection, input and maintenance for data within their functional area.
- Be responsible for authorizing access to applications within their areas.
- Authorize release and use of application data within their areas.
- Establish standards for appropriate business use of data.
- Control data definitions to ensure data conforms to consistent definitions over the life of the data.
- Approve request for access to information by authorized persons



# Records & Information Management

# H a n d b o o k

and assist in the establishment of authorization of data stewards.

- Recommend security classifications and monitor for compliance.
- Serve as a primary source of information on their data (business expert).
- Focus on the integrity of the data by working with the IT and business groups to improve data quality and standardization.

## Some Helpful Definitions

ARS §41-1350 states **records** are: *All books, papers, maps, photographs or other documentary material, regardless of physical form or characteristics... made or received... in connection with the transaction of public business... Records may include computer-based records, voicemail, text messages, email, photographs, motion pictures, video and audio recordings, charts, maps, drawings, plans, micrographics and more*

**Vital records** are those records that are fundamental to the functioning of an organization and necessary to continue its operations immediately under abnormal conditions; these records must be identified and protected so they can be retrieved easily in the event of a disaster, allowing the organization to restore business functions quickly, resume operations, and continue to thrive

An **active record** is needed to perform current operations, subject to frequent use and usually located near the user

An **inactive record** is no longer needed to conduct current business but preserved until it meets the end of its retention period

A **political subdivision** is a quasi-government agency with powers and duties established in the state constitution and in state statute

**Records management** is the maintenance and disposition of records

**"A Metadata Primer," ARMA International**  
[www.arma.org/pdf/articles/md.pdf](http://www.arma.org/pdf/articles/md.pdf)

## Metadata—What is It?

Metadata is data describing context, content, and structure of documents and records and their management through time (ISO 15489-1:2001, 3.12). Literally, metadata is data about data.

## What Does Metadata Do?

Metadata enables the creation, registration, classification, access, preservation, and disposition of records through time and within and across domains. It can be used to identify, authenticate, and contextualize records and the people, processes, and systems that create, manage, maintain, and use them and the policies that govern them.

## Why Is Metadata Important for Records Managers?

Records managers must be able to work with IT staff and vendors when planning and implementing an electronic records management system that meets their organization's goals for improved management of their information assets.

## Metadata About Records

The growth of digital records necessitates a different approach to capturing information about the record. For example, some metadata may still be entered manually, but other metadata can be captured automatically.

## From the Beginning

When records are created or captured, metadata is used to describe the context of the record, the business context, and the agents involved. Metadata is also added to describe the structure of the record so that it is available for use over time. The structure of a record includes both its physical or logical structure and its technical attributes.

## During the Life Cycle

Metadata known as *process metadata* continues to accrue during the life of a record. It is used to document activities that

take place related to the record after its initial capture into the records management system. For example, it defines changes in the logical or physical structure of the record and documents new relationships with other records or aggregations. Both record and process metadata form a record that must be managed for the life of the original record. [See] the article "Why Metadata Matters" in the September/October 2006 issue of *The Information Management Journal*.

## Metadata in a Broader Context

Metadata may be attached to a record by another system for another purpose. It is important to understand metadata in this broader context in order to ensure that appropriate links and relationships are established and metadata are not duplicated or unnecessarily produced. Metadata is also used for

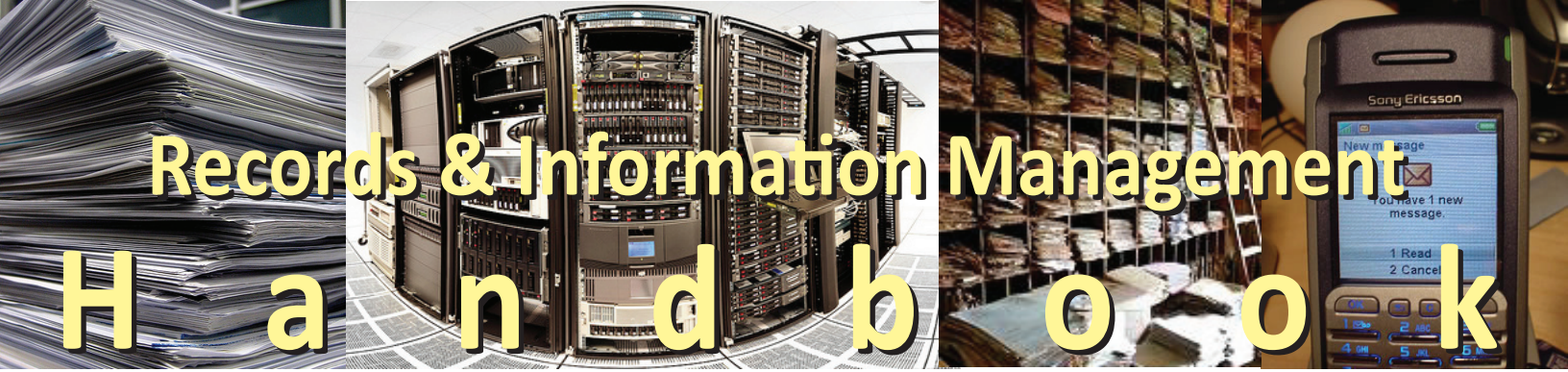
- e-business
- preservation
- resource description
- resource discovery
- rights management

## The Case for Metadata

Metadata can be used to describe an object so that it can be located when needed. Metadata can help organize electronic records, facilitate interoperability across systems, provide digital identification, and support both archiving and preservation.

As the percent of information that is either born or stored digitally grows, concern also grows over our ability to ensure that records will survive and continue to be accessible throughout their life cycle. Many believe metadata is the key to our ability to meet this challenge.

*Arizona's Supreme Court (Lake v. City of Phoenix) has ruled that metadata is considered a public record and is subject to release. Custodians of Records take note. Although the ruling only applies in Arizona, other states may be influenced by the decision.*



# Records & Information Management

# Handbook

**Data** are institutional assets used to support instruction, student services and administrative functions

**Information** is data that has been given value through analysis, interpretation or compilation in a meaningful form

**Metadata** is data describing context, content, and structure of documents and records and their management through time

**Information management** is the practice of analyzing information as a resource of the organization—how that information will be acquired, recorded, organized, stored, retrieved and shared; information management helps to support the effective use of information within the organization

**Records retention** is the maintenance of documents for further use (includes security for confidential information)

**Records disposition** is the destruction of records with lawful authority based on an approved retention and disposition schedule by the Arizona State Library, Archives and Public Records Department

**Disclosure:** To reveal, to make known or to make available for inspection. With the exception of student education records, the majority of records that are created in the MCCC are subject to review

**Non-disclosure:** The act of, or decision made to not disclose a record

Public officials cannot arbitrarily decide what information not to disclose—requests may be denied based upon the requirements established by state and federal law, such as:

- The information is statutorily confidential or privileged (FERPA, HIPAA)
- The information falls within an individual's right to privacy (personal address/phone, social security number)

- It is not in the best interest of the MCCC to release it (to do so would seriously impair performance of duties)
- The records are sealed by Court Order

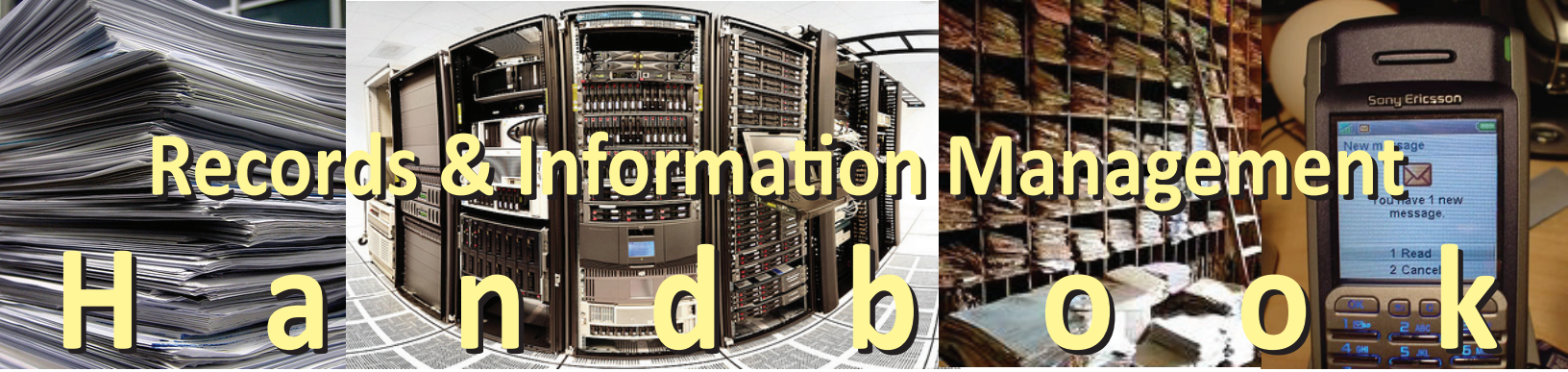
A **legal hold** is a communication issued as a result of current or anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records

A **backup** is a copy of information created as a precaution in case the original is lost or stolen

**Archives** are those records in any medium that, because of their enduring historical or legal value, are retained permanently; for electronic records, archive describes a systematic way to organize and maintain e-records for the duration of their life cycle (a much more comprehensive plan than periodic 'backups')

An **archives program** safeguards and makes accessible the records that must be permanently preserved in order to maintain the organization's institutional memory

**Spoliation** is destroying records while a legal investigation is in action or pending



# Records & Information Management

# H a n d b o o k

## Appendices



# Records & Information Management Handbook

## Appendices

## Frequently Asked Questions

### What types of records are there?

Documents are considered records if they provide value to the MCCCDC in one of the following ways:

- **Administrative:** Records needed to conduct an area's daily business
- **Fiscal:** Records needed to document the audit trail of monies
- **Legal:** Documents that meet specific legal requirements to keep records for a given period of time (found in the Arizona Revised Statutes (ARS), United States Code (USC) and Code of Federal Regulations (CFR)) or any document that shows an agreement between MCCCDC and another entity or that MCCCDC uses to regulate itself by aligning with State/Federal laws
- **Historical:** Documents detailing the conception, creation, operation, and evolution of MCCCDC and its community partnerships
- **Academic / Instructional:** Documents that are used in the process of instruction

### Who is responsible for managing MCCCDC records?

- All Maricopans (whether full-time, part-time, OSO, OYO, temporary or adjunct) are responsible for the documents they create in the course of daily operations
- Faculty, staff and administrators are responsible for knowing about records, records management, information management and records release
- The Office of Public Stewardship provides training and guidance on records management

### What does custodian of record mean?

The party or area at a college or at the district office designated as being responsible for the management of specific records.

The custodian of record will also oversee the review of records prior to release as well as the reproduction of records when requests for copies are made.

### Who is the custodian of record?

It depends on who created it, the purpose and who has jurisdiction over the final product.

### How long do I keep my records?

A retention and disposition schedule approved by the Arizona State Library, Archives and Public Records for Arizona Community Colleges and Districts can be found online at [www.lib.az.us](http://www.lib.az.us).

### How do I dispose of records?

Check to see if there is a pending or imminent litigation, audit or government investigation; if there is a question, do not destroy anything even if the schedule says it's time.

If there is no action pending:

- Non-confidential records may be recycled or thrown away
- Confidential records must be shredded or burned in a manner which ensures continued confidentiality
- Non-record copies should be destroyed at the same time as the record
- A **Certificate of Records Destruction** (see appendices, pg.17) should be prepared and sent to the Arizona State Library, Archive and Public Records Department at the same time the records are destroyed

### What do I do when there is a legal investigation or the possibility of one?

Do not destroy until the legal action, audit or investigation has been released or completed; you may box records and mark for destruction at a later date but they must remain available and accessible.

### How do we secure confidential records? Destroy them?

- Confidential records should be kept in a location that provides limited access to approved individuals (those responsible for maintaining them); this can be done either by securing them in a locked cabinet, locked storage area or off-site in a storage facility that provides limited access to approved individuals only
- Confidential records must be shredded or burned in a manner which ensures continued confidentiality

### Can confidential personnel information be included in adjunct faculty personnel files?

Provided adequate security is provided, yes, with the following exceptions:

- I9 forms
- Medical information (i.e., FMLA requests)

### Can we store our records off-site?

Yes, provided the vendor can adequately guarantee appropriate security for confidential records and relative ease to retrieve records in a timely manner (accessible during normal business hours).

### Are there legal requirements to protect records from fire, smoke, or water damage?

There are legal requirements for MCCCDC to maintain records but no specific laws stating that those records must be stored in fire-proof or water-proof containers; however, it's a good idea to make sure that they are reasonably protected.



# Records & Information Management Handbook

## Appendices

### Who holds the official document when it passes multiple “hands?”

It depends on the document—in most cases, the creator of the document is considered the custodian of record; however, in instances where the document needs to be signed or in which the “original” is considered the official version, that document, wherever it ends up, is the record.

### Are copies considered records?

A copy is not a record, but may become one if the original is destroyed and the copy is not.

### If a paper document is scanned can the electronic file serve as the official record? Can the paper document be destroyed?

It depends on the document, what function it serves and how long the record needs to be preserved.

- If the document serves an historical or legal purpose, the paper document must be preserved (forever, in the case of documents with historical value)
- If the document falls in the administrative or fiscal categories (i.e., invoices) then those may be destroyed once scanned as long as there are no statutes or federal regulations stipulating otherwise

Areas interested in scanning documents need to fill out one of the **Approval of Document Imaging** forms and ensure the vendor responsible for scanning the documents is in compliance (see appendices, pgs. 17-21); there are five versions of the **Approval of Document Imaging** form, with specific criteria based on document content and length of time to be maintained.

Forms can be obtained from the Office of Public Stewardship web at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php).

### How long should adjunct faculty files be maintained?

Personnel files should be maintained for five years from date of separation; contracts should be maintained for three years after completion or cancellation.

- If the information in the files is duplicative of records held elsewhere, the college may dispose of the documents as designated by the department/division (they are considered “copies”)
- If the documents are not housed elsewhere, then the college is responsible for ensuring the records are maintained for the appropriate duration set by the retention schedule

### Are student classroom assignments and projects considered records?

Student classroom assignments and projects are not items subject to a retention schedule or public release—however, they are items that need proper disposal or destruction.

Faculty should:

- Retain up to one year (the length of time a student has to put in a grade grievance) and then destroy as per confidential records OR
- Return assignments/projects to students

### How long past a grant end do files need to be kept? Where should they be stored?

It depends on the type of grant and what part:

- Some parts, like the administrative sections which concern money, budget and allocation, can be discarded after the appropriate time limit (which is usually regulated by the grant funding source)
- Other parts, like the written plan and final project report, are considered historical and will need to be kept forever

### Who is the custodian of grant records?

The grant manager is the custodian of record.

### What records have already been placed on the retention schedule?

The retention schedule for community colleges can be found online at [www.lib.az.us/records/pdf/CommCollRD1.pdf](http://www.lib.az.us/records/pdf/CommCollRD1.pdf).

### Who prepares new Records Retention and Disposition Schedules? Does District have to approve it?

Any area may prepare a schedule in coordination with the Office of Public Stewardship if a schedule does not already exist to meet their needs; the Office of Public Stewardship will need to approve the final version and will work with the Arizona State Library, Archives and Public Records to formalize it for all of the MCCC.

### Who prepares and signs the Certificate of Records Destruction form?

The custodian of record signs and submits the forms directly to the Arizona State Library, Archives and Public Records. Once a Retention Schedule has been approved and implemented the Certificate of Records Destruction form does not need to be reviewed or signed by the Office of Public Stewardship.

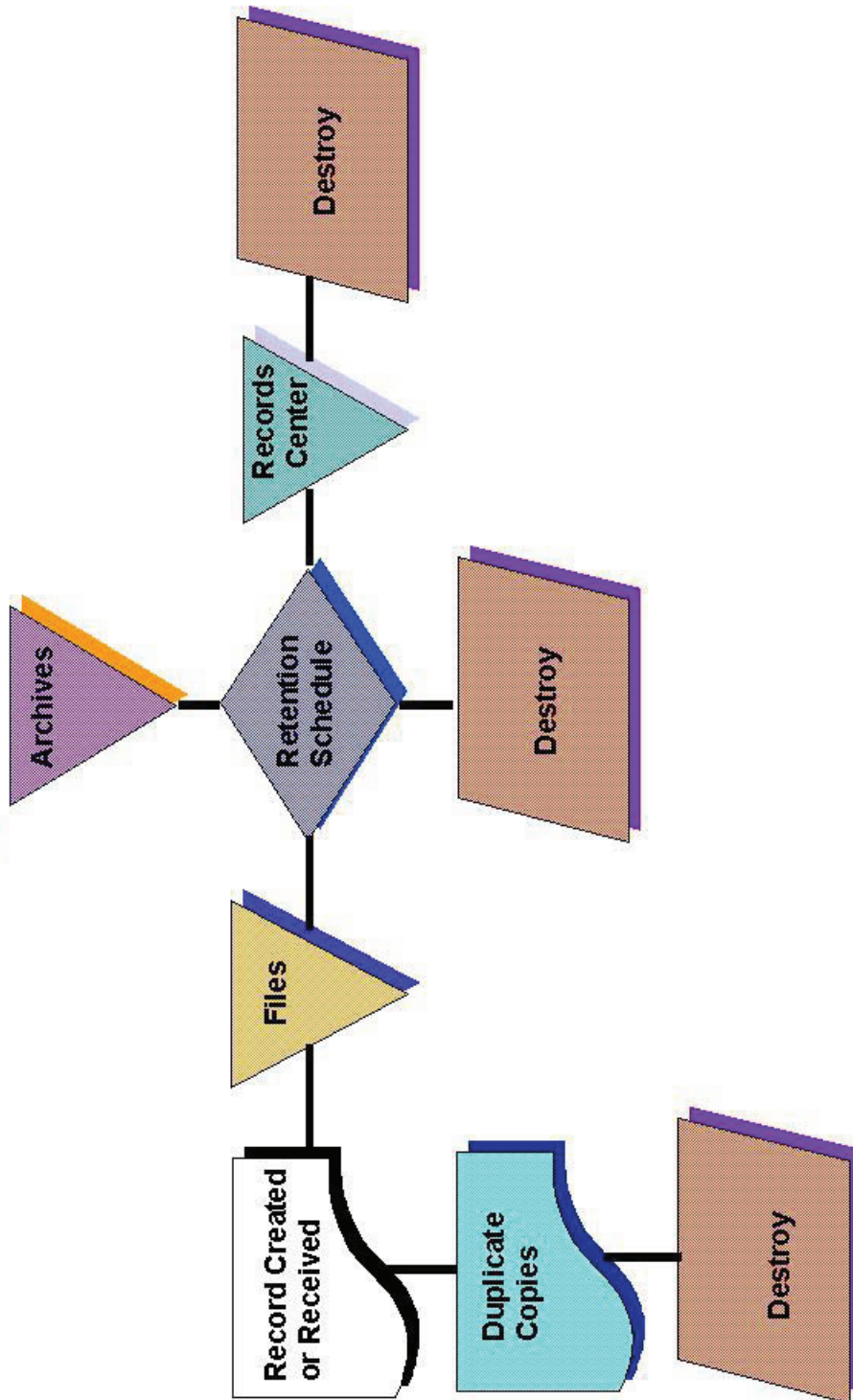
### Are there district-wide services available to help with records destruction?

Several colleges have contracted to outside vendors to securely destroy confidential records or recycle non-confidential records and some colleges have shredders onsite (see appendices, p. 12).

# Records & Information Management Handbook

# Appendices

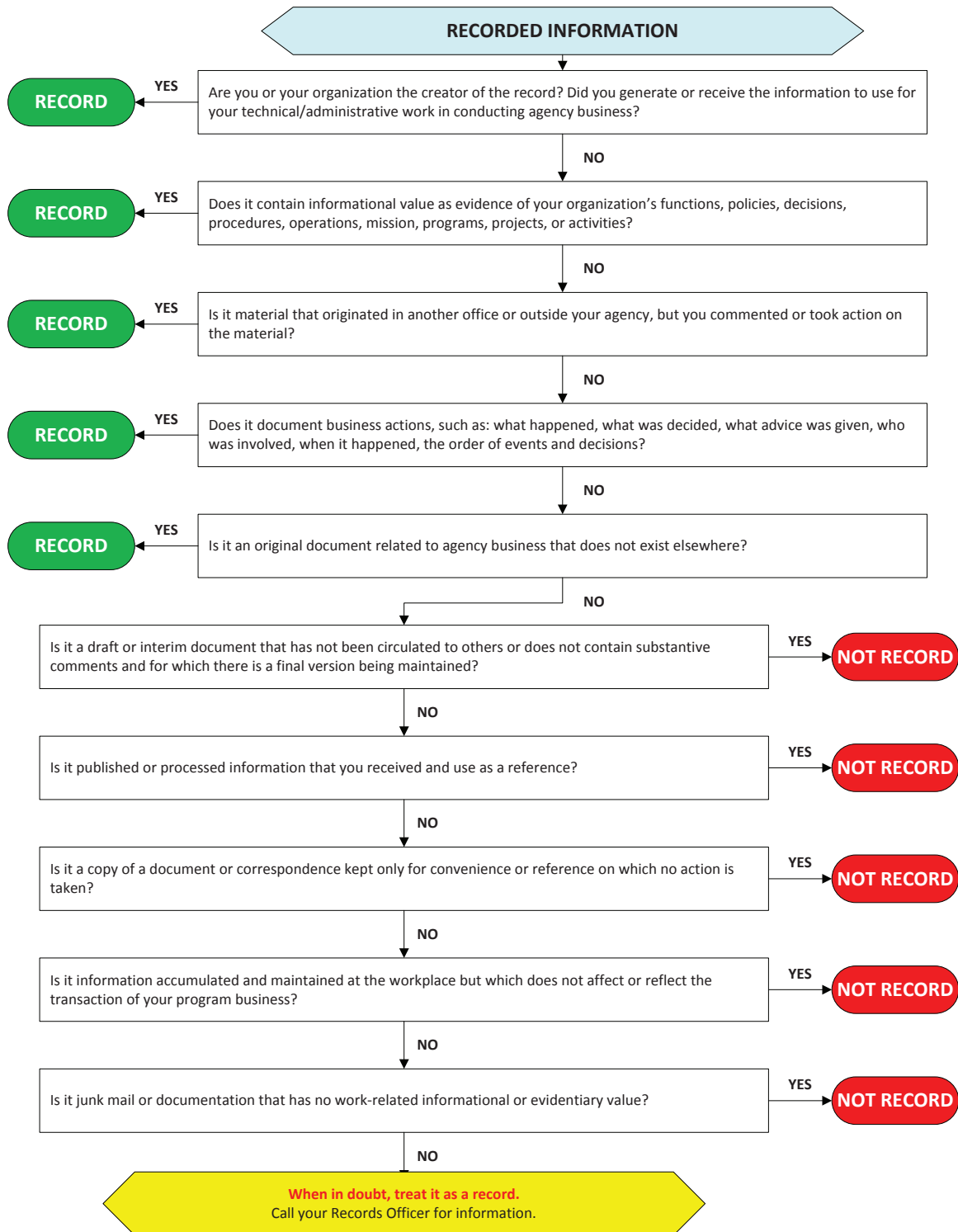
## The Life-cycle of Records



# Records & Information Management Handbook

## Appendices

### Is It A Record?



Courtesy of Anna W. Nusbaum, CRM, Sandia National Laboratories

# Records & Information Management Handbook

## Appendices

### MCCCD Document Destruction Services

Location	College Contact	Vendor	Frequency	Service Availability	Process	Destruction Location
CGCC	Thomas Nicol	No destruction contract. Large shredder housed in Receiving and another in A&R; receiving currently shreds documents for departments on request. Contract with Abitibi for recycling.				
EMCC	Leda Johnson	No destruction contract. Shredder housed onsite; college shreds documents on request. Contract with AZ Center for Blind for paper recycling.				
GWCC	Charles Poure	Arizona Center for the Blind	Bins are rotated out and replaced by request	Continuously available to all	Shred bins (pad locked) and recycle bins located campus-wide	Bins are picked up from the Central Plant (replacing empty for full); vendor shreds documents onsite and recycles shredded materials
GCC	Regis Della-Calce	International Paper	Twice a month; call for additional pick up	Open to all—paper recycling and certified document destruction	Blue bins (shred) and black bins (recycle) padlocked and located campus-wide; campus M&O move full bins to central location	Bins picked up from centralized location (replacing with empty bins); destruction onsite and vendor provides certificate of destruction
MCC	Kurt Conover	Shred-It	First Tuesday of the month	Available to all	20 secure consoles located campus-wide; bins may be relocated at a later date if current locations do not work	Vendor destroys documents onsite and provides certificate of destruction after
PVCC	Jeanette Saxon	International Paper / Weyerhaeuser	Every two weeks or upon request (made through Facilities Services)	Available to all	Locked bins located campus-wide	Bins picked up by vendor and replaced with empty; documents shredded onsite; vendor provides destruction documentation with monthly invoice
PC	Ronnie Elliott Paul DeRose	Cintas (trial period) Assured/TCH	Cintas pickup same as P/W Monthly	65 gal container (A&R, Counseling/Advising/Pu blic Safety, KSC/Student Union and 40" executive console (Admin, HR, Testing, Cont Ed, Fiscal) All PC departments	Limited locations for Cintas bins	Cintas bins are locked, document of destruction submitted onsite after shredding; shredding onsite and can be viewed via video screen (only Fiscal uses this service)
Rio	Todd Simmons	Abitibi Consulting City of Tempe TCH (Security)	Every two weeks	Anyone at Rio	Locked bins provided by vendor located around Rio location(s)	Locked bins are picked up by vendor and replaced with empty bins; documents shredded onsite
SCC	Karen Johnson	Shred-It	Every other week on Wednesday	Available to all	20 secure consoles located campus-wide; contact Karen Johnson or Ray Cruz for additional shredding needs	Vendor destroys documents onsite and provides certificate of destruction after
SMCC	Dzung Tran	International Paper	Once a month, average	Available to all	Giant locked bins located around campus; vendor is called when bins are full and replaces with empty bins	Vendor destroys documents onsite; provides two certificates showing number of pounds recycled
DIST	Darren Stroughter	No destruction contract. Large shredder housed in Receiving and some individual departments contract out.				

Spring 2010

# Records & Information Management Handbook

# Appendices

## RECORDS INVENTORY WORKSHEET



Arizona State Library, Archives and Public Records  
**RECORDS MANAGEMENT DIVISION**

1919 West Jefferson Street, Phoenix, Arizona 85009

Phone: 602-542-3741 • Fax: 602-542-3890 • E-mail: rmd@lib.az.us

Agency Name/Political Subdivision		Organizational Unit	
Office/Sub-Organizational Unit			
Address			Phone Number
Contact Name		Title	
Records Series Name/Title			
		<input type="checkbox"/> Official Copy	<input type="checkbox"/> Access/Use Copy
<b>Records Medium</b>	<input type="checkbox"/> Paper	<input type="checkbox"/> Microfilm	<input type="checkbox"/> Electronic/Computer
	<input type="checkbox"/> Photograph	<input type="checkbox"/> Other	
Description of Records			
<b>Inclusive Dates in File</b>		From:	Through:
<b>Record/File Cut-Off</b>	<input type="checkbox"/> After Calendar Year	<input type="checkbox"/> After Fiscal Year	<input type="checkbox"/> After Event (case closed, project completion, etc.)
<b>Volume of Records (select one)</b>	Cubic Feet	Lineal Inches	File Drawers
<b>Use Frequency of Records</b>	Current Year: references per month	2 through 5 years: references/month	
	Past Year: references per month	Over 5 years: references/month	
<b>Retention</b>			
<input type="checkbox"/> Legal Requirement	years after	Citation	
<input type="checkbox"/> Office Recommendation		years after	
<input type="checkbox"/> Current Retention from Approved Schedule		years after	
<b>Electronic/Computer Media</b>			
Operating System:			
Application Program:			
Data Format:			
<b>Comments</b>			

# Records & Information Management Handbook

## Appendices

### RECORDS RETENTION AND DISPOSITION SCHEDULE



Arizona State Library, Archives and Public Records  
**RECORDS MANAGEMENT DIVISION**  
 1919 West Jefferson Street  
 Phoenix, Arizona 85009  
 Phone: 602-542-3741 Fax: 602-542-3890  
 E-mail: rmd@lib.az.us

**PAGE 1 of**

State Agency Password	Political Subdivision	Agency Name	
Org. Unit/Division		Office	Phone
Address		City	State <b>AZ</b> Zip
Submitted By (Name)		Title	Signature

Pursuant to ARS §41-1351, the following retention periods represent the maximum time records may be kept. Unless records relate to pending or current litigation, or are necessary for an audit, keeping records beyond their retention period is illegal. If you believe that special circumstances warrant the extension of any of these retention periods that records should be kept longer than the period listed below or that any of these record series may be appropriate for transfer to the Archives, please contact the Records Management Division to inquire about a change to the retention period. Only the Records Management Division has the authority to extend records retention periods.

No.	RECORD SERIES	R.S. Code	RETENTION (YR.)			REMARKS (Include start point of retention.)
			Off.	R.C.	Total	
						Supersedes Schedule Dated:

Approved by: <b>X</b> Director, Arizona State Library, Archives and Public Records	Approval Date:
--	----------------

RMC-3 R9/01

# Records & Information Management Handbook

## Appendices

### RECORDS RETENTION AND DISPOSITION SCHEDULE

						PAGE of
State Agency Password		Political Subdivision		Agency Name		
Org. Unit/Division				Office		
<p>Pursuant to ARS §41-1351, the following retention periods represent the maximum time records may be kept. Unless records relate to pending or current litigation, or are necessary for an audit, keeping records beyond their retention period is illegal. If you believe that special circumstances warrant the extension of any of these retention periods records should be kept longer than the period listed below or that any of these record series may be appropriate for transfer should be transferred to the Archives, please contact the Records Management Division to inquire about a change to the retention period. Only the State Library Records Management Division has the authority to extend records retention periods.</p>						
No.	RECORD SERIES	R.S. Code	RETENTION (YR.)			REMARKS (Include start point of retention.)
			Off.	R.C.	Total	
Approved by: <b>X</b> Director, Arizona State Library, Archives and Public Records						Approval Date:

RMC-3 R9/01



# Records & Information Management Handbook

# Appendices



## Arizona State Library, Archives and Public Records

**NOTE:** Request for Minutes to be imaged and source documents are NOT destroyed. Strictly used when Minute records are imaged and used online. Form posted at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php)

### REQUEST FOR DOCUMENT IMAGING OF PUBLIC RECORDS (MINUTES) WHEN THE SOURCE DOCUMENTS ARE NOT DESTROYED

#### REQUEST

The [governing body's name] ("Applicant") requests authorization from the Arizona State Library, Archives and Public Records, in accordance with ARS §41-1348, to scan records described on the attached list and agrees to comply with the following conditions and standards:

1. The only records covered by this agreement are meeting minutes being scanned for dissemination on the Internet.
2. The signed, official copy of the minutes are on paper or microfilm as required by ARS §39-101.
3. The signed, official copy of the minutes will be kept permanently by the Applicant or will be transferred to the Arizona State Library, Archives and Public Records.
4. The Applicant certifies that the images will use the most current versions of TIFF, GIF, JPG, or PDF for the file format and that the images will conform to the following standards. The Library and Archives highly recommends, but does not require, that the online version be in PDF format.
  - Black-and-white text records may be scanned using a bi-tonal scale. If the records' retention period is five years or less they shall be scanned at 200 dpi or greater. Records with a retention period of more than five years shall be scanned at 300 dpi resolution.
  - Black-and-white records containing images or graphics shall be scanned using a 256 gray scale and a resolution of 300 dpi.
  - Color records will be scanned at a minimum 300 dpi resolution and 24 bit color depth.
  - Text files may be compressed using a lossless algorithm. Image files may use a lossy algorithm.
5. The Applicant certifies the system on which the electronic records are stored is backed up and that the backups are routinely verified.
6. The Applicant will institute a quality control process to ensure that all information the scanned versions are legible.
7. A digital copy of the minutes in PDF will be e-mailed to reports@lib.az.us using the subject line "Minutes - Agency or political subdivision name - Date." Copies should be sent as soon as they are mounted to the Web or earlier.

On behalf of [agency or political subdivision]

\_\_\_\_\_  
[Signer's name and title]

\_\_\_\_\_  
Date:

#### AUTHORIZATION

As authorized under ARS §41-1348, the Arizona State Library, Archives and Public Records authorizes the Applicant to reproduce these records using electronic media following these procedures for a period of five years. Failure to comply with these procedures is a violation of ARS §41-1438.

#### RECORDS MANAGEMENT DIVISION

1919 W. Jefferson • Phoenix, Arizona 85009 • Home Page: <http://www.lib.az.us/records/>  
Phone: (602) 926-3815 • FAX: (602) 256-2838 • E-Mail: [rmd@lib.az.us](mailto:rmd@lib.az.us)

An Equal Opportunity Employer



# Records & Information Management Handbook Appendices



## Arizona State Library, Archives and Public Records

**NOTE:** Request for permanent records to be imaged with source documents NOT destroyed. Used if you would like to microfilm Permanent records. Form posted at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php)

### REQUEST FOR MICROFILMING OF PERMANENT PUBLIC RECORDS

#### REQUEST

The [governing body's name] ("Applicant") requests authorization from the Arizona State Library, Archives and Public Records (ASLAPR), in accordance with ARS §41-1348, to microfilm records described on the attached list and certifies the following conditions are true:

1. The records covered by the agreement are to be retained permanently and include (list record series or attach a list for multiple record series):
  
2. The Applicant recognizes that the microfilmed copy of the records may become the official copy, and the applicant will take care to ensure the microfilmed copies are complete and the information is not altered.
3. The Applicant ensures that the microfilmed copies of the records are kept permanently as specified on a records schedule approved by the Arizona State Library, Archives and Public Records. The microfilm will be retained by:  Submitting Agency  Vendor  ASLAPR/RMD
4. The Applicant certifies that the following conditions apply (check all that apply):
  - Filming performed at:  Submitting Agency  Vendor  ASLAPR/RMD
  - Source documents will be:  retained  destroyed by whom:  Submitting Agency  Vendor  ASLAPR/RMD  Archives
  - Microfilmed created using:  Planetary  Rotary  Digital
  - Image Format:  16MM  35MM
  - Copy for Office Use:  Microfilm  Digital
5. The Applicant certifies that a Certificate of Compliance (Form used to certify that the microfilm was processed in accordance with standards published by ASLAPR. See website [www.lib.az.us/records/form](http://www.lib.az.us/records/form) for a copy.) The certificate will be filed annually if the filming is not performed by ASLAPR/RMD.
6. The Applicant certifies that a reduction ratio greater than 24X will not be used.
7. The Applicant will institute a quality control process that includes inspecting at least 10% of all records to ensure that all information on the microfilmed versions are legible. For permanent records where the source documents will be destroyed, 100% of the records must be verified to ensure that all the information on the microfilmed versions is legible.

On behalf of [agency or political subdivision]

\_\_\_\_\_  
[Signer's name and title]

\_\_\_\_\_  
Date:

#### RECORDS MANAGEMENT DIVISION

1919 W. Jefferson • Phoenix, Arizona 85009 • Home Page: <http://www.lib.az.us/records/>  
Phone: (602) 926-3815 • FAX: (602) 256-2838 • E-Mail: [rmd@lib.az.us](mailto:rmd@lib.az.us)

An Equal Opportunity Employer

# Records & Information Management Handbook

# Appendices



Arizona State Library, Archives and Public Records

**NOTE:** Request for documents to be imaged with source documents destroyed (<10 years). Used for records with a total retention period less than 10 years, where you would like to image the records, but still hold on to the paper copies. Form is three pages long, page one listed for reference only. Complete form posted at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php)

## REQUEST FOR DOCUMENT IMAGING OF PUBLIC RECORDS WHEN THE SOURCE DOCUMENTS ARE DESTROYED

### REQUEST

The [**governing body's name**] ("Applicant") requests authorization from the Arizona State Library, Archives and Public Records, in accordance with ARS §41-1348, to scan records described on the attached list and agrees to comply with the following conditions and standards:

1. The records covered by the agreement are not archival records requiring permanent retention and include (list record series, estimated length of time the records must be kept, and retention period or attach a list for multiple record series):
2. The Applicant recognizes that the scanned copy of the records will become the official copy, and the applicant will take care to ensure the scanned copies are complete and the information is not altered.
3. The Applicant will routinely destroy all originals and retain the scanned copies of the records for the period specified on a records schedule approved by the Arizona State Library, Archives and Public Records, and will suspend scheduled destruction of any record potentially responsive to reasonably foreseeable litigation, audit, or investigation.
4. The Applicant certifies that the images will use the most current versions of TIFF, GIF, JPG, or PDF for the file format and that the images will conform to the following standards.
  - Black-and-white text records may be scanned using a bi-tonal scale. If the records' retention period is five years or less they shall be scanned at 200 dpi or greater. Records with a retention period of more than five years shall be scanned at 300 dpi resolution.
  - Black-and-white records containing images or graphics shall be scanned using a 256 gray scale and a resolution of 300 dpi.
  - Color records will be scanned at a minimum 300 dpi resolution and 24 bit color depth.
  - Text files may be compressed using a lossless algorithm. Image files may use a lossy algorithm.
5. The Applicant certifies the system on which the electronic records are stored is backed up and that the backups are routinely verified.
6. The Applicant certifies that the digital images will be appropriately indexed for retrieval based on key data elements in the records (date, name of parties to the records, and other information specific to the particular records series). Indexes will be created for the following fields (list below or on the attached list):
7. The Applicant will institute a quality control process that includes inspecting at least 1% of all records to ensure that all information the scanned versions are legible.
8. The Applicant certifies that the benefits of digitizing these records justifies the costs and is ready to demonstrate that to any concerned party.
9. For state agencies only, the Applicant has submitted a Project Investment Justification (PIJ) to the Government Information Technology Agency (GITA) if required. For more information, see <http://azgita.gov/project%5Fpij%5Fmonitoring/>

### RECORDS MANAGEMENT DIVISION

1919 W. Jefferson • Phoenix, Arizona 85009 • Home Page: <http://www.lib.az.us/records/>  
Phone: (602) 926-3815 • FAX: (602) 256-2838 • E-Mail: [rmd@lib.az.us](mailto:rmd@lib.az.us)

An Equal Opportunity Employer



# Records & Information Management Handbook

## Appendices



### Arizona State Library, Archives and Public Records

**NOTE:** Request for documents to be imaged with source documents NOT destroyed (<10 years). Used for records with a total retention period less than 10 years, where you would like to image the records, and then destroy the paper copies. Form is three pages long, page one listed for reference only. Complete form posted at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php)

#### REQUEST FOR DOCUMENT IMAGING OF PUBLIC RECORDS WHEN THE SOURCE DOCUMENTS ARE NOT DESTROYED

##### REQUEST

The [**governing body's name**] ("Applicant") requests authorization from the Arizona State Library, Archives and Public Records, in accordance with ARS §41-1348, to scan records described on the attached list and agrees to comply with the following conditions and standards:

1. The records covered by the agreement include (list record series, estimated length of time the records must be kept, and retention period, or attach a list for multiple record series):
  
2. The official copy of the records is on paper or microfilm.
3. The Applicant will retain the official, paper copy of the records only for the period specified on a records schedule approved by the Arizona State Library, Archives and Public Records, and will suspend scheduled destruction of any record potentially responsive to reasonably foreseeable litigation, audit, or investigation.
4. The official copy of the records shall be kept by the Applicant, transferred to the State Records Center for storage, or – if permanent – transferred to the State Archives.
5. The Applicant may destroy scanned copies of the records before the approved retention period, and shall destroy the scanned copies at the end of the retention period. Applicant shall seek advice of counsel regarding the destruction of scanned copies of records potentially responsive to reasonably foreseeable litigation, audit, or investigation before destruction of those records.
6. The Applicant certifies that the images will use the most current versions of TIFF, GIF, JPG, or PDF for the file format and that the images will conform to the following standards.
  - Black-and-white text records may be scanned using a bi-tonal scale. If the records' retention period is five years or less they shall be scanned at 200 dpi or greater. Records with a retention period of more than five years shall be scanned at 300 dpi resolution.
  - Black-and-white records containing images or graphics shall be scanned using a 256 gray scale and a resolution of 300 dpi.
  - Color records will be scanned at a minimum 300 dpi resolution and 24 bit color depth.
  - Text files may be compressed using a lossless algorithm. Image files may use a lossy algorithm.
7. The Applicant certifies that the system on which the electronic records are stored is backed up and that the backups are routinely verified.
8. The Applicant certifies that the digital images will be appropriately indexed for retrieval based on key data elements in the records (date, name of parties to the records, and other information specific to the particular records series). Indexes will be created for the following fields:

##### RECORDS MANAGEMENT DIVISION

1919 W. Jefferson • Phoenix, Arizona 85009 • Home Page: <http://www.lib.az.us/records/>  
Phone: (602) 926-3815 • FAX: (602) 256-2838 • E-Mail: [rmd@lib.az.us](mailto:rmd@lib.az.us)

An Equal Opportunity Employer

# Records & Information Management Handbook

## Appendices

**NOTE:** Request for documents to be imaged with source documents destroyed (10+ years). Old style form – used if you would like to image records that have a total retention period greater than 10 years, or if the records have an indefinite retention period, or for multiple records series with various retention periods. Form posted at [www.maricopa.edu/publicstewardship/pr/retention.php](http://www.maricopa.edu/publicstewardship/pr/retention.php)

### REQUEST FOR DOCUMENT IMAGING IMPLEMENTATION



Arizona State Library, Archives and Public Records  
**RECORDS MANAGEMENT DIVISION**  
 1919 West Jefferson Street, Phoenix, Arizona 85009  
 Phone: 602-542-3741 λ Fax: 602-542-3890 λ E-mail: [rmd@lib.az.us](mailto:rmd@lib.az.us)

<b>Authorized pursuant to A.R.S. §41-1348</b> (Violation of this statute is a misdemeanor crime.)		New req.	Revised	Date Submitted	
		<input type="radio"/>	<input type="radio"/>		
State Agency <input type="radio"/>	Political Subdivision	Agency Name			
Org. Unit/Division		Office	Phone		
Address		City	AZ	Zip	
Submitted By (Name)	Title	Signature X			
<b>DESCRIPTION OF RECORDS TO BE IMAGED: (Include record series name as it appears on the retention and disposition schedule and list various documents included in the series.)</b>					
Record Series				Retention (yrs.)	
<b>MICROFILM/FILM-BASED IMAGING</b> (Briefly describe the filming application in the "Comments" area of this request.)		<input type="radio"/>	<b>ELECTRONIC/DIGITAL IMAGING</b> (Complete the balance of this request.) <input type="radio"/>		
<b>STUDIES PERFORMED:</b>		<input type="radio"/> Feasibility (attach copy)	<input type="radio"/> Cost/Benefit (attach copy)	<input type="radio"/> P.I.J. (attach copy)	
<b>LIST HARDWARE BELOW:</b>		<b>LIST SOFTWARE BELOW:</b>			
<b>MIGRATION/EXIT PLAN FOR LONG TERM RECORDS (Retention of 10 years or more)</b>					
<input type="radio"/> Migration/Exit Plan Adopted	<input type="radio"/> 5% – 10% System Cost annually Budgeted	<input type="radio"/> Vendor Source Code in Escrow			
<b>IMAGING SYSTEM HAS ABILITY TO COMPLETELY PURGE/DESTROY/EXPUNGE OBSOLETE RECORDS (IMAGES).</b>				<input type="radio"/> Yes	<input type="radio"/> No
<b>OPEN SYSTEM ARCHITECTURE</b>				<input type="radio"/> Yes	<input type="radio"/> No
<b>NONPROPRIETARY HARDWARE AND SOFTWARE</b>				<input type="radio"/> Yes	<input type="radio"/> No
<b>IMAGE FORMAT</b>		<input type="radio"/> TIFF with Std. Headers <input type="radio"/> Group 3 <input type="radio"/> Group 4 <input type="radio"/> Other:			
<b>IMAGE RESOLUTION</b>		<input type="radio"/> 200 dpi <input type="radio"/> 300 dpi <input type="radio"/> 400 dpi <input type="radio"/> Other:		<input type="radio"/> Bimodal <input type="radio"/> Grayscale	
<b>INDEXING</b>		<input type="radio"/> O.C.R. <input type="radio"/> Manual <input type="radio"/> Number of fields:		<b>BACKUP MEDIA:</b>	
<b>COMMENTS:</b>					
Approved by:				Approval Date	
Director, Arizona State Library, Archives and Public Records				Expires on (Approval date + 5 years)	

RMC-2 R04/02



# Records & Information Management Handbook

## Appendices

### Management and Protection of Data

#### Purpose

This section of the Maricopa Data Access and Appropriate Use Best Practice explains and defines the standards, behaviors and recommendations for management and protection of Confidential Data aimed at minimizing the potential risks of data compromise which may exist as a consequence of sharing Confidential Data between and among Maricopa entities or as a result of routine client/server interaction. The Management and Protection of Data define and describe the following:

- objectives for securely storing and disseminating “confidential data.”
- objectives and standards for applications using the “primary authentication credentials.”
- objectives for the applications accessing the data or directories replicated from the data.

#### Scope

All employees and agents of Maricopa, anyone working on behalf of Maricopa and any persons with authorized access to confidential data. This best practice applies to all forms and circumstances of access, sharing, use, manipulation, replication and retention of Confidential Data within and between Maricopa business units and/or Colleges or individuals.

#### Definitions

**Data Steward** – Data Stewards are those persons authorized by a college president or vice chancellor or through a process of formal request and approval from a Custodian of Record to access, manage, manipulate and disseminate confidential data. Data Stewards differ from Custodians of Record in the following ways:

- They are responsible to Custodians of Record for the approval to gain access to data unless they are delegating previously approved responsibilities of stewardship to an eligible person
- They have no responsibilities for the data regarding response to subpoenas or other legal inquiries
- The justification for access to data generally centers around the development or creation of a system, process or application

**Delegate** – The formal process of transferring all or a portion of the responsibilities of stewardship to another person. Recognition that delegation occurred requires that the intent to transfer such responsibilities to another person be made in writing specifying the date of the transfer and the specific responsibilities inherited by the delegate. It also requires a written acknowledgement by the delegate of those specific responsibilities he or she is accepting as of a specific date.

**Service Provider** – Service Provider means any person or entity that receives, maintains, processes or otherwise is permitted access to

confidential information through its provision of service on behalf of Maricopa or any of its subdivisions.

#### Principles of Management and Protection, Stewardship and Responsibility: Limitations and Responsibilities

##### Data Stewards

By reason of organizational role, or through the request and subsequent granting of permission by custodian of record, data stewards are charged with the careful and responsible management of confidential data entrusted to their care. It is the responsibility of the data steward to be informed and knowledgeable of practices and standards related to data or information resource security. As it may be required by his or her job responsibilities, the stewards of confidential data should be able to demonstrate that he or she has taken steps beyond basic actions to mitigate the potential for data compromise or loss resulting from the malicious activity of others.

##### Delegation of Responsibility

The data steward may delegate any or all responsibilities related to being a data steward to anyone he or she may have a functionally dependent or supervisory relationship with related to managing, developing systems for or reporting against confidential data. The delegate of the data steward should have the operational capacity to carry out the duties and responsibilities of stewardship that have been granted to them. The delegate should also be made aware of this administrative regulation and comply with any procedure regarding the formal acknowledgement of their responsibilities to appropriately use and safeguard Confidential Data. Persons to whom delegation of responsibility has been granted have the same duty as the data steward to adhere to the requirements of this regulation.

##### Data Stewards With Partial or Limited Technical Infrastructure Responsibility

As a function or limitation of his or her job responsibility, a data steward may not possess responsibility for assessing or correcting vulnerabilities in the information technology infrastructure at the campus or site where an application or system under their care may reside. In such a case, the data steward should make an effort to inform the person or persons responsible for the security of that infrastructure or vice chancellor of any serious vulnerability that may affect the security of the applications, processes or data under his or her care. Upon receipt of such notification, the person or persons responsible for the information technology infrastructure should take appropriate action to assess the accuracy of such a report and take any appropriate corrective action.



# Records & Information Management Handbook Appendices

## Responsibilities of Data Stewardship and Use

Approved data stewards should ensure that confidential data entrusted to their care are appropriately safeguarded based upon the following security objectives. Adherence to these objectives also includes the introduction and periodic orientation of applicable staff to the requirements of this best practice.

These security objectives apply, as appropriate, to all users, developers and administrators or anyone who has access to confidential data including Custodians of Record.

### Source Document

[www.maricopa.edu/its/Process%20-%20DI%20Data%20Mgmt.pdf](http://www.maricopa.edu/its/Process%20-%20DI%20Data%20Mgmt.pdf)



# Records & Information Management Handbook

## Appendices

### Principals of Acceptable Use

Access to confidential data may be granted as necessary to complete work assignments for the benefit of Maricopa or any of its affiliates or subdivisions. This access may include varied types of information systems such as development, core production or shadow systems.

Acceptable use and access to confidential data may also include varied types of media such as paper records, printed reports, computer screens, electronic storage devices and network transmission.

Information not classified as public should be protected and should not be disclosed without authorization. Unauthorized access, manipulation or disclosure of such information may constitute a breach of security.

All users of data are expected only to collect and maintain data as needed to effectively conduct Maricopa business as required by job duty or specifically authorized assignment. Sensitive Personal Information should not be collected unless it is appropriate and relevant to the approved purpose for which it was collected. Sensitive Personal Information should be collected, to the extent practicable, from the individual directly and not from other sources. Where Sensitive Personal Information is obtained from other sources, a record should be maintained of those sources from which the Sensitive Personal Information was obtained.

There should be no Sensitive Personal Information collected or maintained which has not been approved by the appropriate Custodian of Record. All users having access to Confidential Data should formally acknowledge their understanding of the level of access they have been granted and their responsibility to maintain the confidentiality of the data to which access has been granted.

**Source Document**

[www.maricopa.edu/its/Process%20-%20DI%20Acceptable%20Use.pdf](http://www.maricopa.edu/its/Process%20-%20DI%20Acceptable%20Use.pdf)



# Records & Information Management Handbook

## Appendices

### Reasonable Protection

#### Storing Data

Confidential data should be stored or made available in such a way that access is restricted and authorization required prior to presenting such data to authorized persons or processes. Authorization should be verified at least once at the beginning of each access session and may include but is not limited to the use of access credentials such as a secure username and password, biometric reading or other forms of user identification/credentials such as cryptographic keys. Steps beyond basic actions may include but are not limited to the use of firewalls, restricted or private networks, physical access security or other techniques or systems designed to stop or mitigate the success of unauthorized attempts to obtain data.

#### Access Credentials

Access Credentials should be used to uniquely identify a process or person and should not be made public. Access credentials not belonging to or representative of a person are also considered confidential data. Passwords or similar credential components should not be viewable while being entered or at any time after entry. System passwords or the answers to challenge questions should be saved immediately in a secure repository in encrypted form based upon industry standards.

#### Prohibited Credentials

- Complete Social Security Number or National ID
- complete birth date
- a value equal to the username or sign-on credential

#### Transport of Data

Confidential Data during either physical or electronic transport should not be viewable or otherwise accessible to anyone other than the intended recipient. Steps beyond basic actions may include but are not limited to the use of network transport encryption techniques or any system, protocol or process that is aligned with industry standards which has the intent of mitigating or limiting the usability of such data in the event it was intercepted while in transport.

#### Gathering Displaying Data

Confidential data while being gathered or displayed should leave no residue such as in web browser caches or any other electronic or manual input device. Data gathering techniques should include steps to mitigate the affects of user impersonation, or other electronic data entry exploits intended to obtain data through errant or malicious entries of instructions, commands or queries in an electronic input form. Steps beyond basic actions may include but are not limited to the inclusion of field edits, logical result validation or any other techniques and or software intended to limit the effectiveness or potential of common data input exploits.

#### Disposal of Electronic Data Systems

Disposal of electronic data systems or storage devices that may have contained confidential data should be accomplished in such a way as to mitigate the possibility that Confidential Data previously stored on such devices could be retrieved or otherwise obtain by unauthorized persons.

#### Administrative Data Users

Maricopa employees who have functional responsibility to develop applications, reports or technical systems that use confidential data are responsible to safeguard such data while it is in their care or possession. Care or possession includes access to and or control of physical documents or any other form of information generated as a logical or direct consequence of interfacing with administrative systems and reports including any data extracted from administrative systems regardless of medium, wherein confidential data is included. As applicable, users should adhere to the standards of data security described above.

#### Due Diligence of Service Providers

The adequacy of the service provider's system of safeguarding information should be determined prior to Maricopa or any of its subdivisions entering into a contractual relationship with the service provider. Maricopa or any of its subdivisions should not contractually engage a service provider who cannot demonstrate that they have a system to safeguard the confidential information that they manage, receive or transfer on behalf of Maricopa. Depending on the service provider, Maricopa may wish to review the service provider's audits, summaries of its test results for security or other internal and external evaluations. Maricopa or any of its subdivisions should not enter into contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

#### Service Provider Agreements

All contracts with service providers should include a privacy clause which requires the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party. Contracts should, when appropriate, include the requirement that in addition to the Maricopa insurance requirements for service agreements, the service provider indemnify Maricopa from financial loss or expense resulting from any requirement to notify victims of security breaches and/or any related cost for credit monitoring or general communication related to the breach of such data.

#### Source Document

[www.maricopa.edu/its/Process%20-%20DI%20Reasonable%20Protection.pdf](http://www.maricopa.edu/its/Process%20-%20DI%20Reasonable%20Protection.pdf)



# Records & Information Management Handbook

## Appendices

## Student Records

### MCCCD Administrative Regulation 2.5.3

#### 1. Definitions

For the purposes of this policy, the Maricopa County Community College District has used the following definition of terms.

- A. "College" includes all colleges, educational centers, skill centers and District office.
- B. "Educational Records" are any record (in handwriting, print, tapes, film, or other media) maintained by the college or an agent of the college which is directly related to a student, except:
  - i. A personal record kept by a staff member, if it is kept in the personal possession of the individual who made the record, and information contained in the record has never been revealed or made available to any other person except the maker's temporary substitute
  - ii. An employment record of an individual whose employment is not contingent on the fact that he or she is a student, provided the record is used only in relation to the individual's employment
  - iii. Records maintained by the colleges security unit, if the record is maintained solely for law enforcement purposes, is revealed only to law enforcement agencies of the same jurisdiction and the security unit does not have access to education records maintained by the community college.
  - iv. Alumni records which contain information about a student after he or she is no longer an attendant of the community college and the records do not relate to the person as a student

#### 2. Fees

If a copy(ies) of a portion or all of the records in a student's file is requested, the custodian of the records may charge a fee for copies made. However, the willingness or ability to pay the fee will not effectively prevent students from exercising their right to inspect and review (under supervision of a college employee) their records. A fee will not be charged to search for or to retrieve records. Standard fees for printing and duplication services will apply.

#### 3. Annual Notification

Students will be notified of their further rights annually by publication in the college catalog and/or the student handbook:

##### Rights of Access to Educational Records

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. These rights are:

- A. The right to inspect and review the student's education records within 45 days of the day the college receives a request for access.

Students should submit to the college admissions and records department written requests that identify the record(s) they wish to inspect. The college official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the college official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

- B. The right to request the amendment of the student's education records that the student believes to be inaccurate or misleading.

Students may ask the college to amend a record that they believe is inaccurate or misleading. They should write the college official responsible for the record, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading.

If the college decides not to amend the record as requested by the student, the college will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

- C. The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.

One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interest. A school official is defined as a person employed by the college or District in an administrative, supervisory, academic, or support staff position (including law enforcement unit and health staff); a person or company with whom the college or District has contracted (such as an attorney, auditor, or collection agent); a person serving on the Governing Board; or a person assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

Upon request, the college discloses education records without consent to officials of another school in which a student seeks or intends to enroll.



# Records & Information Management Handbook

## Appendices

D. The right to file a complaint with the US Department to Education concerning alleged failures by the college to comply with the requirements of FERPA.

The name and address of the Office that administers FERPA is:  
Family Policy Compliance Office  
US Department of Education  
400 Maryland Ave., S.W.  
Washington, DC 20202-4605

#### 4. Student Directory

A Maricopa community college may release directory information about any student who has not specifically requested the withholding of such information. Students who do not want directory information released may so indicate during the admissions process or notify the Office of Admissions and Records.

At any Maricopa community college, directory information is defined as a student's name, address, telephone number, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees and awards received, dates of attendance, part-time or full-time status, most recent previous educational agency or institution attended by the student, college within the Maricopa Community Colleges where the student has been enrolled, photograph of student, and electronic mail address.

#### 5. Use of Education Records for Advisement Purposes

All colleges within the Maricopa Community Colleges have access to the computerized degree audit program. During the advisement process, each student may have his or her academic record reviewed for coursework taken at any of the District's colleges or centers. The institution retains the right to exercise discretion in determining the release of directory information.

#### 6. Disclosure to Parents

In accordance with federal law, college officials may disclose educational records to parents of minors or to parents of a student who have established the student's status as a dependent according to the Internal Revenue Code of 1986, section 152, without the written consent of the student.



# Records & Information Management Handbook

## Appendices

### Electronic Communications Retention and Records Requests

#### MCCCD Administrative Regulation 4.15

##### Introduction

The Maricopa County Community College District (MCCCD) regards electronic messaging and voice communications as vehicles for delivery of information and not as primary mechanisms for the retention and archival of such information. Reasonable efforts will be taken to maintain the integrity and effective operation of the electronic message and voice systems. These systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information.

As a public organization, Arizona law establishes that communications sent electronically by MCCCD personnel may constitute “correspondence” and, therefore, may be considered as records subject to retention and public inspection.

##### Retention and Recovery

Electronic mail will be retained on tape for one month after the date of a system backup. It is the responsibility of the electronic mail user to determine what information is essential to his or her official activities and should be retained or archived in his or her e-mail account, and retain that information locally.

Voice mail communications may be erased or otherwise destroyed after taking the required action. Voice mail backups will be retained for one month after the date of a system backup.

Upon formal request, every attempt will be made by MCCCD to recover the contents of electronic communications from tape backups that fall under this retention schedule. For an electronic message to be available on a backup tape, it must reside in a mailbox or file on MCCCD’s central service system for 24 hours.

#### Requests for Copies and Inspection of Electronic Communications and Hardware

If there is a local hardware or system failure, employees may request that electronic communications created by them or written directly to them be restored from backup. All requests for copies or searches for electronic communications created and maintained by other account users of MCCCD’s electronic communication systems and that may involve a specific content or topic area must be reviewed and authorized by the General Counsel.

MCCCD expects to cooperate fully and expeditiously with law enforcement or government officials when information from its computing resources is required for investigative purposes. Information that is requested by a lawfully issued administrative summons or judicial order, including search warrants and subpoenas, must be submitted to the Office of General Counsel. Requests made by members of the general public should be directed to the District ombudsperson.

After review and authorization by the General Counsel, requests for copies of electronic communications will be forwarded to ITS security services. ITS security services will comply with the request and coordinate retrieval of the information within seven business days.

*Adopted through the Administrative Regulation approval process on February 24, 2004*

#### References

The schedules of retention and dispersal for community colleges in Arizona are approved and monitored by the Arizona State Library, Archives and Public Records. Questions about any of this information may be directed to:

Arizona State Library, Archives  
and Public Records

State Records Management Center

1919 West Jefferson Street

Phoenix, AZ 85009

(602) 542-3741 / (602) 542-3890 FAX

[www.lib.az.us](http://www.lib.az.us)

Office of Public Stewardship

Maricopa Community Colleges

District Office

2411 West 14th Street

Tempe, AZ 85281-6942

(480) 731-8880/8882 / (480) 731-8819 FAX

[www.maricopa.edu/publicstewardship](http://www.maricopa.edu/publicstewardship)

