Records & Information Management Handbook

M A R I C O P A C O M M U N I T Y C O L L E G E S®

February 2012
# Table of Contents

- **Objectives** ................................................................. 3
- **What is a Record?** ...................................................... 3
- **What is Not a Record?** ............................................... 3
- **Records and Information Management** ......................... 3
- **Public Records** .......................................................... 3
- **Value of MCCCD Records** .......................................... 3
- **Managing Records** ..................................................... 4
- **Custodian of Record** .................................................. 4
- **Retention Schedules** .................................................. 4
- **Disposition of Records** ............................................... 4
- **Creating a New Retention Schedule** .............................. 4
- **Considerations for E-Documents** ................................. 4
- **Electronic Imaging of Paper** ........................................ 5
- **Data Management** ...................................................... 5
- **Access, Use and Protection of Data** ............................... 5
- **Authorized Access** .................................................... 5
- **Acceptable Use** .......................................................... 5
- **Reasonable Protection** ............................................... 5
- **Custodian of Record Accountability** .............................. 5
- **Some Helpful Definitions** ............................................ 6
- **A Metadata Primer** .................................................... 7

## Appendices

- **Frequently Asked Questions** ........................................ 9
- **Lifecycle of Records** .................................................. 11
- **Is It A Record?** .......................................................... 12
- **MCCCD Document Destruction Services** ......................... 13
- **Records Inventory Worksheet** ....................................... 14
- **Records Retention Schedule** ........................................ 15
- **Certificate of Records Destruction** ................................ 17
- **Imaging Requests** ........................................................ 18-19
- **Minimum Standards for Digital Imaging or Scanning Textual Documents** ........... 20
- **Management & Protection of Data** .................................. 21
- **Principles of Acceptable Use** ........................................ 22
- **Reasonable Protection** ............................................... 23
- **Student Records** ........................................................ 24
- **Retrieval, Disclosure, and Retention of Records** .................. 26
- **Retrieval, Disclosure, and Retention of Records FAQ** ............. 28
Records and Information Management (RIM) for MCCCD

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 are 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 requests 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 Community College District (MCCCD), the types of records and information the MCCCD has, 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
Records management is the maintenance and disposition of a record throughout its lifecycle. Data are electronic institutional assets used to support instruction, student services, and administrative functions. According to ARMA International (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 “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 MCCCD is a political subdivision of the state, so many records created by the MCCCD are considered public records. If a public records request is made, MCCCD 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, HIPAAA);
• 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 MCCCD to release it (to do so would seriously impair performance of duties); or
• the records are sealed by Court Order.

Value of MCCCD Records
Documents and data are categorized according to their value to the MCCCD 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 MCCCD and another entity or that MCCCD 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 MCCCD 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 MCCCD? 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. 14) 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.

### 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 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 destroyed 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. 17) should be prepared by the custodian of record 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 pending, 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. 14) 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 MCCCD-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 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 archive 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 created two imaging requests for those documents which are suitable for scanning. 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. 18-19):

- Request for Document Imaging of Public Records or
- Request for Microfilming of Permanent Public Records

The Minimum Imaging Standards for Digital Imaging or Scanning Textual Documents (see appendices, pg. 20) gives the minimum standards and formats required for digital imaging or scanning.

Data Management
Following are MCCCD 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)

Access, Use, and Protection of Data
Maricopa County Community College District (MCCCD) recognizes its affirmative and continuing need to protect confidential employee and student data and to maintain the confidentiality of that data.

The MCCCD 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.

Data are institutional assets used to support instruction, student services and administrative functions. While access and use of data is essential to accomplishing the MCCCD’s institutional mission, it requires the observance of critical standards to safeguard individuals’ rights that are protected by state and federal laws or MCCCD regulations. Therefore, MCCCD 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
MCCCD’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. 21) for more information.

Acceptable Use
All employees and agents of MCCCD and anyone working on behalf of MCCCD 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. 22) for more information.

Reasonable Protection
All employees and agents of MCCCD and anyone working on behalf of MCCCD are charged with the protection of MCCCD 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
- 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. 23) 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 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

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
“A Metadata Primer,” ARMA International
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.

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.
Frequently Asked Questions

What types of records are there?
Documents are considered records if they provide value to the MCCCD 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 MCCCD and another entity or that MCCCD uses to regulate itself by aligning with State/Federal laws
- **Historical**: Documents detailing the conception, creation, operation, and evolution of MCCCD and its community partnerships
- **Academic / Instructional**: Documents that are used in the process of instruction

Who is responsible for managing MCCCD 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 MCCCD 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.

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 and what function it serves.

- 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 a Request for Document Imaging of Public Records or Request for Microfilming of Permanent Public Records form and ensure the vendor responsible for scanning the documents is in compliance (see appendices, pgs. 18-19).

Forms can be obtained from the Office of Public Stewardship web at www.maricopa.edu/publicstewardship/pr/rimresources.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 cancelation.
- 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.

**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 MCCCD.

**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. 13).
Is It A Record?

RECORDED INFORMATION

Are you or your organization the creator of the record? Did you generate or receive the information to use for your technical/administrative work in conducting agency business?

YES

NO

Does it contain informational value as evidence of your organization’s functions, policies, decisions, procedures, operations, mission, programs, projects, or activities?

YES

NO

Is it material that originated in another office or outside your agency, but you commented or took action on the material?

YES

NO

Does it document business actions, such as: what happened, what was decided, what advice was given, who was involved, when it happened, the order of events and decisions?

YES

NO

Is it an original document related to agency business that does not exist elsewhere?

YES

NO

Is it a draft or interim document that has not been circulated to others or does not contain substantive comments and for which there is a final version being maintained?

YES

NOT RECORD

NO

Is it published or processed information that you received and use as a reference?

YES

NOT RECORD

NO

Is it a copy of a document or correspondence kept only for convenience or reference on which no action is taken?

YES

NOT RECORD

NO

Is it information accumulated and maintained at the workplace but which does not affect or reflect the transaction of your program business?

YES

NOT RECORD

NO

Is it junk mail or documentation that has no work-related informational or evidentiary value?

YES

NOT RECORD

NO

When in doubt, treat it as a record. Call your Records Officer for information.

Courtesy of Anna W. Nusbaum, CRM, Sandia National Laboratories
## MCCCD Document Destruction Services

<table>
<thead>
<tr>
<th>Location</th>
<th>College Contact</th>
<th>Vendor</th>
<th>Frequency</th>
<th>Service Availability</th>
<th>Process</th>
<th>Destruction Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGCC</td>
<td>Thomas Nicol</td>
<td>No destruction contract. Large shredder housed in Receiving and another in A&amp;R; receiving currently shreds documents for departments on request. Contract with Abitibi for recycling.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMCC</td>
<td>Leda Johnson</td>
<td>No destruction contract. Shredder housed onsite; college shreds documents on request. Contract with AZ Center for Blind for paper recycling.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GWCC</td>
<td>Charles Poure</td>
<td>Arizona Center for the Blind</td>
<td>Bins are rotated out and replaced by request</td>
<td>Continuously available to all</td>
<td>Shred bins (pad locked) and recycle bins located campus-wide</td>
<td>Bins are picked up from the Central Plant (replacing empty for full); vendor shreds documents offsite and recycles shredded materials</td>
</tr>
<tr>
<td>GCC</td>
<td>Regis Della-Calse</td>
<td>International Paper</td>
<td>Twice a month; call for additional pick up</td>
<td>Open to all—paper recycling and certified document destruction</td>
<td>Blue bins (shred) and black bins (recycle) padlocked and located campus-wide; campus M&amp;O move full bins to central location</td>
<td>Bins picked up from centralized location (replacing with empty bins); destruction offsite and vendor provides certificate of destruction</td>
</tr>
<tr>
<td>MCC</td>
<td>Kurt Conover</td>
<td>Shred-It</td>
<td>First Tuesday of the month</td>
<td>Available to all</td>
<td>20 secure consoles located campus-wide; bins may be relocated at a later date if current locations do not work</td>
<td>Vendor destroys documents onsite and provides certificate of destruction after</td>
</tr>
<tr>
<td>PVCC</td>
<td>Jeanette Saxon</td>
<td>International Paper / Weyerhaeuser</td>
<td>Every two weeks or upon request (made through Facilities Services)</td>
<td>Available to all</td>
<td>Locked bins located campus-wide</td>
<td>Bins picked up by vendor and replaced with empty; documents shredded offsite; vendor provides destruction documentation with monthly invoice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cintas (trial period)</td>
<td>Cintas pickup same as IP/W</td>
<td>65 gal container (A&amp;R, Counseling/Advising/Public Safety, KSC/Student Union and 40” executive console (Admin, HR, Testing, Cont Ed, Fiscal)</td>
<td>Limited locations for Cintas bins</td>
<td>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)</td>
</tr>
<tr>
<td>PC</td>
<td>Ronnie Elliott</td>
<td>Assured/TCH</td>
<td>Monthly</td>
<td>All PC departments</td>
<td>Contact PC Employee Services to 1) get key to central locked bin location or 2) meet an employee who will unlock site; large deliveries can use PC Receiving to pick up</td>
<td>Locked bins are picked up by vendor and replaced with empty bins; documents shredded offsite; special pick-up may be scheduled for big jobs</td>
</tr>
<tr>
<td></td>
<td>Paul DeRose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rio</td>
<td>Todd Simmons</td>
<td>Abitibi Consulting City of Tempe TCH (Security)</td>
<td>Every two weeks</td>
<td>Anyone at Rio</td>
<td>Locked bins provided by vendor located around Rio location(s)</td>
<td>Locked bins are picked up by vendor and replaced with empty bins; documents shredded offsite</td>
</tr>
<tr>
<td>SCC</td>
<td>Karen Johnson</td>
<td>Shred-It</td>
<td>Every other week on Wednesday</td>
<td>Available to all</td>
<td>20 secure consoles located campus-wide; contact Karen Johnson or Ray Cruz for additional shredding needs</td>
<td>Vendor destroys documents onsite and provides certificate of destruction after</td>
</tr>
<tr>
<td>SMCC</td>
<td>Dzung Tran</td>
<td>International Paper</td>
<td>Once a month, average</td>
<td>Available to all</td>
<td>Giant locked bins located around campus; vendor is called when bins are full and replaces with empty bins</td>
<td>Vendor destroys documents offsite; provides two certificates showing number of pounds recycled</td>
</tr>
<tr>
<td>DIST</td>
<td>Darren Strother</td>
<td>No destruction contract. Large shredder housed in Receiving and some individual departments contract out.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Spring 2010
# 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

<table>
<thead>
<tr>
<th>Agency Name/Political Subdivision</th>
<th>Organizational Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office/Sub-Organizational Unit</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Phone Number</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Title</td>
</tr>
</tbody>
</table>

| Records Series Name/Title | ☐ Official Copy | ☐ Access/Use Copy |

## Records Medium
- ☐ Paper
- ☐ Microfilm
- ☐ Electronic/Computer
- ☐ Photograph
- ☐ Other

| Description of Records          |                                      |

## Inclusive Dates in File

<table>
<thead>
<tr>
<th>From:</th>
<th>Through:</th>
</tr>
</thead>
</table>

## Record/File Cut-Off
- ☐ After Calendar Year
- ☐ After Fiscal Year
- ☐ After Event (case closed, project completion, etc.)

## Volume of Records (select one)

<table>
<thead>
<tr>
<th>Cubic Feet</th>
<th>Lineal Inches</th>
<th>File Drawers</th>
</tr>
</thead>
</table>

## Use Frequency of Records

<table>
<thead>
<tr>
<th>Current Year:</th>
<th>2 through 5 years:</th>
<th>Past Year:</th>
<th>Over 5 years:</th>
</tr>
</thead>
<tbody>
<tr>
<td>references per month</td>
<td>references/month</td>
<td>references per month</td>
<td>references/month</td>
</tr>
</tbody>
</table>

## Retention

| ☐ Legal Requirement | years after | Citation |
| ☐ Office Recommendation | years after |
| ☐ Current Retention from Approved Schedule | years after |

## Electronic/Computer Media

<table>
<thead>
<tr>
<th>Operating System:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Program:</td>
</tr>
<tr>
<td>Data Format:</td>
</tr>
<tr>
<td>Comments:</td>
</tr>
</tbody>
</table>

RMC-9 R5/2004
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

<table>
<thead>
<tr>
<th>No.</th>
<th>RECORD SERIES</th>
<th>R.S. Code</th>
<th>RETENTION (YR.)</th>
<th>REMARKS</th>
</tr>
</thead>
</table>

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.

Supersedes Schedule Dated:

Approved by:
X
Director, Arizona State Library, Archives and Public Records

RMC-3 R9/01
# RECORDS RETENTION AND DISPOSITION SCHEDULE

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.

<table>
<thead>
<tr>
<th>No.</th>
<th>RECORD SERIES</th>
<th>R.S. Code</th>
<th>RETENTION (YR.)</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Approved by:

X

Director, Arizona State Library, Archives and Public Records

RMC-3 R9/01

RIM Handbook Appendices Page 16
REPORT/CERTIFICATE OF RECORDS DESTRUCTION

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

□ STATE AGENCY  □ POLITICAL SUBDIVISION

DATE

AGENCY NAME

ORGANIZATIONAL UNIT

PHONE

ADDRESS

CITY

AZ

ZIP

LIST RECORDS DESTROYED

RECORD SERIES

DATES COVERED

FROM

THRU

ESTIMATED VOLUME *

CERTIFICATE

The above records have been destroyed so as to render them totally useless.

DESTROYED BY (NAME)

TITLE

SIGNATURE

DATE

*Volume of paper records is estimated in cubic feet to the nearest whole number. Volume of digital records may be stated by the estimated memory volume it consumed.
REQUEST FOR DOCUMENT IMAGING OF PUBLIC RECORDS

REQUEST

The ________________________________________________ [agency or political subdivision] requests authorization from the Arizona State Library, Archives and Public Records, in accordance with ARS §41-151.16, to scan records described on the attached list and agrees to comply with the following conditions and standards:

See Attached Retention Schedule – circled records series will be imaged

CHECK ALL OF THE CATEGORIES THAT APPLY BELOW AND READ SPECIAL INSTRUCTIONS FOR THE LENGTH OF RETENTION AND DISPOSITION OF ORIGINALS THEN COMPLETE THE REST OF THE FORM

A. ______ PERMANENT RETENTION

a. I UNDERSTAND AND AGREE THAT ARCHIVAL (PERMANENT) RECORDS APPROVED FOR SCANNING UNDER THIS REQUEST CANNOT BE DESTROYED UNLESS THERE IS A MICROFILM COPY THAT MEETS OR EXCEEDS STATE STANDARDS.

________________________________
Applicant Signature

B. ______ RETENTION TEN YEARS OR UNDER SOURCE DOCUMENTS DESTROYED

a. 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.

b. 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.

C. ______ RETENTION TEN YEARS OR UNDER SOURCE DOCUMENTS NOT DESTROYED

a. The official copy of the records is on paper or microfilm.

b. The Applicant will retain the official 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.

c. The official copy of the records shall be kept by the Applicant or transferred to the State Records Center for storage.
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/rimresources.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):

   See Attached Retention Schedule – circled records series will be imaged

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 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 1% 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.
Minimum Standards for Digital Imaging or Scanning Textual Documents

Standards for additional formats to follow.
For further information please call the State Archives (602) 926-3720

Scan Resolution assumes 100% scan ration and original 8.5”x11”

<table>
<thead>
<tr>
<th>Textual Documents With or Without Illustrations in Text</th>
<th>Retention of records 20 years or less</th>
<th>Retention of Records 21 years to permanent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minimum Scan Resolution</td>
<td>Save As File Format</td>
</tr>
<tr>
<td>Clean, high contrast documents with smallest character of 1.0mm or larger, text only</td>
<td>200 dpi</td>
<td>PDF TIF (group 4 or 6)</td>
</tr>
<tr>
<td>Documents with handwritten notes/markings, low contrast, half-tone illustrations, photographs or poor legibility</td>
<td>300 dpi grayscale</td>
<td>PDF TIF (group 4 or 6)</td>
</tr>
<tr>
<td>Documents and items where color is important for accurate representation</td>
<td>300 dpi 24-bit color</td>
<td>JPEG PDF</td>
</tr>
</tbody>
</table>

Your scanning request must be approved by the Records Management Division, Arizona State Library, Archives and Public Records. Please contact Jerry Lucente-Kirkpatrick at: 602-926-3820.

Note: Careful attention must be paid to metadata, file naming schemas, directory structure, versioning, naming of derivative files, long term storage, migration, backup and disaster recovery to ensure “faithful reproduction” and access to the document over time.

“Faithful digital reproductions are digital objects that are optimally formatted and described with a view to their quality (functionality and use value), persistence (long-term access), and interoperability (e.g. across platforms and software environments). Faithful reproductions meet these criteria, and are intended to accurately render the underlying source document, with respect to its completeness, appearance of original pages (including tonality and color), and correct (that is, original) sequence of pages. Faithful digital reproductions will support production of legible printed facsimiles when produced in the same size as the originals (that is, 1:1).” (Quoted from: Digital Library Federation’s Benchmark for Faithful Digital Reproductions of Monographs and Serials at www.diglib.org/standards/bmarkfin.htm and supported by Federal Agencies Initiative Still Image Working Group’s Technical Guidelines for Digitizing Cultural Heritage Materials www.digitizationguidelines.gov/guidelines/FADGI_Sill_Image-Tech_Guidelines_2010-08-24.pdf.)

Note:
• These are general recommendations. Considerations such as original document size, quality, legibility, image characteristics (spatial resolution, signal resolution, and color mode) and intended use will be needed to be taken into account digital reproductions.
• Scan resolution assumes 100% scan ratio (1:1).
• This table provides the minimum guidelines for digitization. Use the appropriate standard in the table above that most closely matches the overall content of the items you wish to digitize.
• Quality control will need to be performed consistently throughout the process to ensure quality of scans. Check with Records Management Division for quality control requirements.
• Digitization thresholds need to be adjusted based on contrast of original document. You must evaluate the digital output quality to verify that the digitized version accurately represents the content of the original document.
• You must evaluate the legibility of the scans regardless of meeting standards. Meeting minimum standards does not imply legibility of the digital reproduction.

These standards are based, in part, on the following:

Last Updated: February 13, 2011 by LR
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.

**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-%20Dir%20Data%20Mgmt.pdf

RIM Handbook Appendices Page 21
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
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
2.5.3 Student Records

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. Records Request
   Official verification of educational records is issued by the Admissions and Records Office/Office of Student Enrollment Services.

3. 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.

4. 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.

   D. Upon request, the college discloses education records without consent to officials of another school in which a student seeks or intends to enroll.
   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
5. **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.

6. **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.

7. **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.
Retrieval, Disclosure, and Retention of Records

MCCCD Administrative Regulation 4.15

Introduction
The Maricopa County Community College District (MCCCD) is subject to the State’s broad public records law, obligating it to produce records under a public records request and to retain those records in a consistent manner throughout MCCCD.

That same expectation of consistency in public records production, retention and disposal applies to records that are requested through a subpoena, warrant, judicial or administrative order, litigation discovery document or as part of an MCCCD grievance, investigation or review. So, while MCCCD is composed of 10 colleges, two skill centers, several centers and the District Office, its ability to retrieve, disclose and retain public records must be subject to a single set of standards and one process.

Centralized Authority
Under this administrative regulation, the authority to manage MCCCD public records is centralized in the Manager of the Office of Public Stewardship (Manager). This authority extends to responding to or overseeing the response to public records requests in compliance with State law and establishing standards for the retention, retrieval, disclosure and disposal of public records.

The authority also extends to having access to the electronic records of an MCCCD employee or a Governing Board member under the procedures and narrow circumstances specified in this regulation. Under those circumstances and procedures, the Manager and the Vice Chancellor of Information Technology or his designee/supervisee are authorized to access those electronic records using third-party technology tools that MCCCD has purchased. The Vice Chancellor may, after conferring with the Manager and General Counsel, authorize access on a case-by-case basis to a non-District Office information technology employee on the request of the College President who supervises that employee justifying the need for access, the scope of the access, and the duration that access is needed.

Public Records Generally
Under Arizona’s public records law, MCCCD must make records in its custody open for public inspection by any person, and to provide any person with copies on request. That mandate includes records that reside in electronic form. MCCCD also must preserve those records according to the standardized retention and disposition schedules approved by the Arizona State Library, Archives and Public Records applicable to Arizona Community Colleges and Districts (Retention Schedule). See Arizona Revised Statutes §§39-121 et seq.

MCCCD employees and Governing Board members should presume that all work-related records that they produce during work hours as well as communications and attachments sent or received electronically in the performance of duties relating to MCCCD (whether through an MCCCD technology resource or other technology resource) are public records. The MCCCD General Counsel and the Manager will make the final determination of whether something is a public record or not under the law.

Individual Employees’ and Governing Board Members’ Responsibility to Comply
Arizona State Library, Archives and Public Records places the responsibility to manage public records in compliance with the law on the individual MCCCD employee or Governing Board member. It does not matter whether the record is in paper or electronic form. The responsibility is the same—on the individual.

Where a record is only in electronic form and resides within MCCCD’s technology resources, an electronic record that an employee deletes may still be retained through the normal operation of those resources. However, the law as interpreted by the Arizona State Library, Archives and Public Records does not place primary responsibility for retention of those records on MCCCD technology resources. The primary responsibility for managing each individual employee’s or Governing Board member’s electronic records is squarely on that employee or member. The Arizona State Library, Archives and Public Records has made that clear despite potential practical barriers to easy compliance, such as a limitations on memory within an MCCCD employee’s computer.

Note that it is a violation of MCCCD’s Administrative Regulation 4.4, “Technology Resource Standards,” for an employee to delete or alter an electronic public record in violation of public records retention requirements, or in anticipation of receiving or after receipt of a public records request, subpoena, a request for records as part of an MCCCD grievance, investigation or review, or other lawful request for the record.

The standards for retaining and disposing of records are discussed in more detail under the next section of this regulation.

Understanding and Applying Record Retention and Disposal Standards
The official Retention Schedule is available at: www.lib.az.us/records/documents/pdf/CommColIRD1.pdf

The Arizona State Library, Archives and Public Records’ “rule of thumb” places public records into four categories based on their content: administrative, legal, fiscal research, or historical. Records of historical value must be retained permanently. For records in the other three categories, the length of time that the record must be maintained and then disposed of varies. Additionally, the description of the types of records in the Retention Schedule is by general subject matter (such as “EEO/ Affirmative Action” or “Fiscal/Business Operations”), and not by the descriptor “administrative,” “legal” or “fiscal research.” A single record may have content that places it under more than one category with differing retention requirements. In those cases, the employee or Governing Board member should keep it for the longest duration specified in the Retention Schedule.

The Retention Schedule requires public employees and officers to maintain electronic records in their original form. A paper copy of the electronic record does not comply with the standards in the Retention Schedule. All public employees and governing board members, including those for MCCCD, have an obligation to retain electronic records even when they are leaving public employment or as a member of a public governing board.
Information is available on MCCCD’s Public Records website to assist employees and Governing Board members in making retention determinations. See www.maricopa.edu/publicstewardship/pr/schedule.php. If an employee or Governing Board member has questions about the time period for which a record should be retained, he or she may contact the Manager for assistance.

The policy of Maricopa is to use its best efforts to comply with the Retention Schedule in a consistent and systematic manner. Compliance requires cooperation and diligence, particularly when it comes to retention of electronic records. The daily volume of electronic records produced, the speed in which they are created and sent, and the storage limitations on MCCCD servers make adhering to the Retention Schedule complicated.

For electronic records, this administrative regulation recommends a general retention/disposal standard for employees and Governing Board members of one year from the creation or receipt of the record. During that time, the employee or Governing Board member is encouraged to review the Retention Schedule to determine if a shorter or longer period of time is required. If the employee or Governing Board member believes that retention beyond a year is required, he or she may forward the electronic record to the following website: [URL to be inserted].

Finally, MCCCD employees and Governing Board members are reminded not to retain records beyond the period of time that the Retention Schedule requires.

**District Office and College Records Officers**

To implement the standards specified in this administrative regulation, each College President shall appoint a Records Officer from among the College’s Vice Presidents to coordinate public records requests, subpoenas, warrants, judicial or administrative orders, litigation discovery documents, or records as part of a grievance, investigation or review (collectively, “requests”) with the Manager. The Records Officer shall notify the Manager of requests made directly to the College and be responsible for preparing a response plan for records residing at the College. The plan should include determining the possible location of the records, College staff to assist with the search and retrieval of the records, the scope of the search, the need for search confidentiality and a projected completion date for the search. For records requests that are initiated through the Manager’s office or that seek records at more than one College, the Records Officer shall develop the plan with the Manager. The Manager shall serve as the Records Officer for the District Office.

The Manager will maintain a list of records requests. Either the Manager or the Records Officer shall, to the extent practicable, keep a copy of the entire set of records produced pursuant to a request.

MCCCD employees or Governing Board members who seek access to MCCCD public records for reasons other than MCCCD business shall be required to submit a public records request as though they are an outside party.

**Timeliness of Request Response**

Arizona’s Public Records Law states that “[t]he custodian of [public] records shall promptly furnish such copies . . .” See Arizona Revised Statutes §39-121.01-D-1. The Records Officer and, where applicable, the Manager shall be responsible for determining a reasonable date by which the search and copying of documents should be complete, based on criteria such as the size and scope of the request and the availability of staff to conduct those activities. However, it is the policy of MCCCD to proceed with due diligence to accommodate requests as quickly as circumstances permit and, in the case of public records requests, subpoenas, warrants and discovery documents, to comply with the time standards specified in the law, by law enforcement, by judicial order, or by rules of court. An MCCCD employee or Governing Board member who believes that a timeline established by the Records Officer and the Manager is unreasonable shall immediately advise them in writing of the reasons and recommend an alternative plan for review by the Records Officer and the Manager.

**Record Holds**

The Chancellor, Manager or General Counsel may direct that some or all MCCCD employees and Governing Board members place a hold on deleting records relating to particular subjects or issues. Once the Chancellor issues directive, employees and Governing Board members are prohibited from deleting or altering the records that are subject to the hold until the Chancellor, Manager or General Counsel advises that the hold is lifted. Situations in which holds are likely to occur include but are not limited to litigation involving MCCCD and law enforcement investigations.

**Access to Electronic Records**

Investigative Access. There are circumstances under which the General Counsel, the Manager or a College President needs to have access to an employee’s e-mail communications or other electronic records without advising the employee. Those situations generally occur when: MCCCD is served with a subpoena, a warrant, or judicial order that requires confidentiality; confidentiality is directed by a law enforcement agency; or the employee is subject of an MCCCD grievance, investigation or review that the Manager determines, after initial review, requires access.

If a College President believes that he or she needs access to an employee’s e-mail communications or other electronic records, the President shall discuss the matter with the Manager. Only the Manager may request, and only the General Counsel or an Assistant General Counsel acting in the General Counsel’s absence may authorize, access to an employee’s e-mail and electronic records for investigative purposes. Authorization shall be in writing and define the scope of the access required to conduct the review. As specified in the section of this administrative regulation entitled “Standard for Search Capabilities Regarding Electronic Records,” each College’s e-mail system shall authorize the Manager and the Vice Chancellor of Information Technology or his or her designee/supervisee to have direct access to conduct a search without the need to rely on the information technology staff of the College. The standards for search capabilities shall apply regardless of the centralized ability of the Manager and the Vice Chancellor to conduct a search as described in the section under this administrative regulation entitled “Centralized Authority.”

If the requirement for confidentiality is removed, the Manager may but is not obligated to advise the employee that his or her e-mails or other electronic records were accessed. An employee who believes that his or her e-mail or electronic records were illegally accessed shall notify the General Counsel in writing of the reasons. The General Counsel’s determination regarding the legality of access shall be conclusive.
Operational Access. There may be operational circumstances that require access to an MCCCD employee's electronic records in the absence of the employee, such as when the employee is on vacation or ill. Like paper documents on an employee’s desk or files, electronic records belong to MCCCD and need to be available for business purposes. In those instances, the College President or the Chancellor shall complete the form available at Appendix ____ and submit it for approval to the Vice Chancellor for Information Technology or his or her designee for approval. The College President shall provide a copy of the approved form to the employee whose electronic records were accessed.

Access to Former Employees’ Records. All records should be maintained according to value and the respective retention schedule. An employee who resigns or retires from his or her position at MCCCD shall contact his/her direct supervisor about preserving his or her electronic records before his or her departure. Those records shall be transferred to a storage device and provided to the supervisor.

**Standard for Search Capabilities Regarding Electronic Records**

All electronic records systems serving Maricopa shall be capable of doing the following, which are minimum standards for access:

- Automated archival process for messages and documents sent and received with the capability of implementing different archiving standards by type of record as specified in the retention and disposition schedules approved by the Arizona State Library, Archives and Public Records
- Destruction according to that same retention schedule (life cycle of item per schedule)
- Capability to search for words or terms within headers and message or document text, and to
- Assurance that messages and other records cannot be changed or deleted (message integrity)
- Access to the Manager and the District Office’s Information Technology Department to search, retrieve and delete under the circumstances specified in this administrative regulation
- Audit to determine who logs in, searches, retrieves, deletes
- Capacity, longevity, security, recovery
- Ability of MCCCD to maintain ownership of the records
- Ability to place holds on records subject to a request
- Pull records within a reasonable period of time after the initiation of the search command
- Restore records in their original format and to the individual level, with restoration occurring ____ minutes of the initiation of the restore command
- Preservation of past records and well as new ones when switching to a different communications system

The Chancellor or the Chancellor’s designee shall have the authority to approve an electronic records system that does not have one or several of the capabilities specified above when the unique needs of a Maricopa entity require use of that system, and safeguards are in place to assure that use of the system will permit the recording and retrieval of records as required by law.

**Requests for Copies**

A Maricopa employee may request that electronic communications created by him or her or written directly to him or her be restored from backup in the case of a hardware or system failure where the electronic record has passed through the District Office’s server. All such requests must be reviewed and authorized by the General Counsel.

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.

*AMENDED through the Administrative Regulation approval process, June 27, 2011*

*ADOPTED through the Administrative Regulation approval process, February 24, 2004*
Retrieval, Disclosure, and Retention of Records Frequently Asked Questions

As a public sector organization, the Maricopa County Community College District frequently responds to records requests in accordance with Arizona Public Records Law. In order to facilitate the process and ensure a prompt and thorough search, the MCCCD is piloting new software that will establish a centralized approach for the search, retrieval, and disclosure of records to be conducted at the District level when public records requests, subpoenas, or warrants that involve electronic communications have been presented to any Maricopa location as part of litigation, grievance, investigation, or general records request. The present method either relies on each email user or college IT to search and retrieve email messages. The new software will allow for consistent searches to be objectively performed and determinations to be made as to what is/is not subject to release in accordance with applicable laws and Governing Board Policy.

How will the search and disclosure of emails work?
The Office of Public Stewardship (OPS) has been identified as the custodian on behalf of each college and the district office to perform searches of email accounts and produce the records when a college or the District is responding to a public records request, subpoena, warrant, judicial or administrative order, litigation, discovery request, or when locations must produce email records as part of a grievance, investigation, or review. In addition, the OPS will coordinate the search with a records officer appointed by each College President or Vice Chancellor.

What is the responsibility of employees? First, be mindful that college/district email accounts are to be used for college/district business. While the Technology Resource Standards administrative regulation allows for limited incidental use of computer and technology resources, the creation of personal or non-business related communications with your college/district email account is strongly discouraged.

Likewise, as public sector employees, college/district email accounts should be used when conducting Maricopa business. Personal email accounts should not be used as a means or an attempt to circumvent the disclosure of public records.

Second, retain email messages according to their “value.” Not all messages are created equal. Having a set time limit to retain all messages (i.e. 30 days, 60 days, 90 days, etc.) is not the proper way to save email. Communications should be retained based upon their content; either by their administrative, legal, fiscal, or historical value. For faculty, communications with students are not considered public records, yet they have an instructional or academic value and should be retained for the time period allowed for a student to grieve a grade.

How do I retain records according to their value? The Arizona State Library, Archives and Public Records (ASLAPR) defines four categories of value, to which we have added a fifth since we are an educational institution:

• **Administrative**: Records that are needed to conduct an office’s daily business (i.e., procedures manuals, retention schedules, memos, reports)
• **Fiscal**: Records needed to document the audit trail of monies (i.e., budget records and expenditure reports, wage and salary, benefits)
• **Legal**: Specific legal requirements to keep records for a given period of time can be found in the Arizona Revised Statues (ARS), United States Code (USC), and Code of Federal Regulations (CFR) or any document that shows an agreement between MCCCD and another entity or that MCCCD uses to regulate itself by aligning with State/Federal laws (i.e., contracts and agreements, administrative regulations, Governing Board policies)
• **Historical**: Any document that details the conception, creation, operation, and evolution of MCCCD and its community partnerships (i.e., Governing Board minutes, student records, chancellor/president papers, college history, photos, plans, architectural renderings)
• **Academic / Instructional**: Documents 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 a retention schedule or release, a general rule of thumb is to either return projects to students or to retain them through the time period in which a student has to submit a grade grievance.

First, determine the value of the record using the definitions above.

Second, based on the value, determine how long the records must be kept. The only category of records that should be maintained forever is “historical.” All other records have a definite date for deletion. Retention schedules are posted online at [www.maricopa.edu/publicstewardship/pr/schedule.php](http://www.maricopa.edu/publicstewardship/pr/schedule.php).

Finally, file records according to their retention time frame. Do not leave them in your inbox. You may organize files within those broad categories, but the important thing is to keep what needs to be kept (for as long as the timeframe on the applicable schedule).

Does this mean I have to create 100+ folders for each individual time frame identified on the retention schedules? Am I expected to memorize the retention schedules?

No, you can streamline things by creating 3-5 categories, i.e., one year, three year, five year, 10+ years, and permanent/historical. To keep it simple, most day-to-day operational emails will have a limited administrative value (less than one year). Documents that fall in the historical category have been posted at [www.maricopa.edu/publicstewardship/pr/historical.php](http://www.maricopa.edu/publicstewardship/pr/historical.php). These are the only documents that should be maintained forever, all others should be deleted at the appropriate time. It shouldn’t be too difficult to determine the time frames for the types of records that you deal with on a daily basis. Plus, you can always contact the Office of Public Stewardship for help.

Why are you asking me to do this when I’m already so busy with my day-to-day work load?
The retention of records according to value has always been a requirement for public sector organizations. With the increased use and reliance on technology, this is a reminder that regardless of format, we are still required to retain public documents according to a schedule. Arizona Public Records law has one of the broadest definitions of what constitutes a record and most of the documents produced...
for MCCCD (or related to MCCCD even if created on a personally-owned device) are subject to release upon request. As electronic messages and other documents memorialize our operations, the public has a right to access those records. The proper maintenance and retention of public records is part of responsible stewardship.

**Can I print the email and then delete it so I don’t have to worry about this stuff?**
A printed email is still an email. If a records request is received for email records, the printed email would be subject to release. If you print the email and delete the original … it wouldn’t be readily captured as part of the District’s search of electronic messages. While it would be permissible to retain hard copies, as part of the records search, the Office of Public Stewardship would also request that the respective email user submit any hard copy email messages documents that would fall within the scope of the request.

**Can I put everything in one file and let the new system handle the disposition for me? I think all records should be kept forever (or, conversely, not kept at all).**
Every email does not have the same value and the management of it should be handled as with as any other work assignment. But no one will be monitoring your use of the archiving system so if you choose to do this it might only come to light in the event of a legal action or public records request. However, depending on the nature of the request, you may be held accountable if it’s discovered. Destroying public 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 includes public records requests).

**What if the email has personal information included (i.e., health information, social security number, employee ID, etc.)?**
The following information will not be shared in the event of a public records request. Such information will be redacted (blacked-out) or it will not be disclosed at all:

- Information that is statutorily confidential or privileged (FERPA, HIPAA)
- Information that falls within an individual’s right to privacy (personal address/phone, social security number, employee/student ID, etc.)

- Information that is not in the best interest of the MCCCD to release (to do so would seriously impair performance of duties)
- Records that are sealed by Court Order

**Can’t IT take care of this for me?**
Each department, division, or college should review the retention schedules for community colleges in order to determine the timelines for how long to keep. The new archiving system will allow the MCCCD to move toward a more automated system of retention and disposition of emails, but it still requires your input.

**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 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

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