

## **TITLE: RECORDS AND INFORMATION MANAGEMENT**

### **POLICY STATEMENT:**

Red Deer College has a Records and Information Management Program in place to manage the lifecycle (creation/receipt, use, maintenance, storage and disposition) of all College records, regardless of the media or format of the records, and to ensure compliance with legislative mandates.

### **PURPOSE:**

The Records and Information Management Program provides controls for the protection and security of records throughout the lifecycle while assisting in providing efficient systems for access to the information by College staff or other authorized parties. The Program:

- is compliant, effective and efficient,
- provides the ability to ensure regulatory compliance to local, provincial and federal legislation,
- provides a high degree of information usability for staff,
- allows information to flow seamlessly within the organization with necessary access restrictions in place, and
- integrates into processes and is not a process unto itself.

### **SCOPE:**

This Policy covers all records and information, in all media and formats, in the custody or under the control of the College and is to be followed by all College staff and third parties using College records and information.

### **PRINCIPLES:**

Decisions related to the Records and Information Management Program are based on seven key operating principles:

1. Responsiveness - respond quickly, completely and professionally to requests for assistance with records issues.
2. Accuracy - each component of the Program provides checks and balances to support the accuracy and authenticity of College records.
3. Consistency - policies, guidelines and standards are applied equally to all business units.
4. Simplicity - straightforward solutions are implemented as appropriate to meet the need.
5. Flexibility - unique situations are provided with unique solutions.
6. Responsible handling - All information handled by the Records Management team is managed in a manner that ensures confidentiality/privacy, provides reasonable protection to the information, is open and accountable, and is respectful of individual rights.
7. Red Deer College complies with the Post Secondary Learning Act and other relevant legislation such as the Freedom of Information and Protection of Privacy Act.

## **DEFINITIONS:**

**Destruction** - Records are considered destroyed when they are unreadable and unrecoverable.

**Disposition:** Permanent transfer, destruction or permanent archiving of records. Records are considered permanently transferred when the College has sent the records to a third party and does not retain any copies, in any format. Records are considered archived when the College sends the records to a recognized archival facility and does not retain any copies, in any format or segregates the records in an internal archive level storage space.

**Format:** Different methods media can be structured with for record storage. Examples of paper formats include single pages, bound pages, maps, plans, and books. Examples of electronic formats include word processing documents, slide shows, databases, GIS maps, and web pages.

**Litigation Hold and Release:** Notifications from Legal Counsel suspending the process of routine destruction or deletion of Records and Transitory Records when it is determined that the Records or Transitory Records may be relevant to threatened or pending litigation or government investigations. A Litigation Hold Release is a notification from the Legal Department that the suspension of routine destruction or deletion is no longer in effect.

**Media:** Includes paper, electronic, tapes (audio and video), film, and microform (film and fiche).

**Organizational Records Structure:** Framework that expands on the Retention and Disposition Schedule with additional information for each record type, such as: security classification, FOIP identification, vital records, and classification.

**Record and Information:** All information, documents and data, regardless of media or format, which demonstrate a business transaction or decision by the College.

**Records Inventory:** Database/spreadsheet of the College's record types.

**Records Liaison:** A representative in each business area that acts as the coordinator for records based activities and is the "go to" support for issues like record classification, storage or retrieval.

**Records Management Team:** Comprised of the CIO with overall responsibility for Records Management and the Data & Information Management Specialist who handles the daily activities of Records Management and Information.

**Record Taxonomy (aka Classification):** Organizational structure for College records.

**Retention and Disposition Schedule:** Authoritative document designed in accordance with legislative, operational and historical requirements for the retention and final disposition of all records within RDC. The Schedule is a component of the Organizational Records Structure.

**Sensitive Information** - Information that is protected against unwarranted disclosure for legal or ethical reasons, for issues pertaining to personal privacy, for proprietary considerations, for potential harm to the College's business reputation or relations, or that contain information not

approved for consumption beyond the College's operations. Examples of sensitive information may include: contracts (prior to finalization), personnel information, records related to investigations (both internal and external), and business development strategies that name specific opportunities (prior to exploration or involvement in the opportunity).

**Staff Member:** All employees at RDC including faculty, staff and administrative employees.

**Tax Holds and Tax Hold Releases** - are managed by the Finance Department suspending the process of routine destruction or deletion of Records and Non-Records when it is determined that the Records or Non-Records may be relevant to open tax matters. The Finance Department manages the process whereby the Tax Hold is released and the Records and Non-Records can be destroyed or deleted according to the Retention and Disposition Schedule and the Records Taxonomy.

**Transitory Records:** Records that are not substantive, do not add value to a business transaction or simply contain no business information. Example: drafts of minutes are considered records until a final version is completed (the final copy then becomes the record). Specific examples of Transitory Records include:

- **Unsolicited items:** personal development course brochures, retail sales flyer/catalogues (ex: retail catalogue).
- **Notes:** phone messages (once the message is received and none of the notes are required for future reference or action), notes taken on a recording device such as a Dictaphone (once they've been added to the master file).
- **Duplicates and blanks:** additional copies of documents (where a master is maintained and the copy has not been altered to form a new original), blank unused forms (no information added), blank storage media (ex: tapes, CDs, portable drives) (only considered blank if a low level formatting has been completed or the media has never been used).
- **Reference/library material:** materials collected from third party sources (ex: books, newspapers, magazines, web pages, third party presentation materials) that are not required to support specific records.

**Security:** Security of records includes administrative, physical and technical controls that reduce the risk of accidental or intentional loss, damage, access, distribution, destruction or theft.

#### **GUIDELINES:**

1. Administrative controls include:
  - 1.1. Guidelines for facility environmental controls related to physical records storage.
  - 1.2. Creation of a key information listing that includes the record type and its value rating, as part of the corporate Emergency Response and Business Resumption Plan.
  - 1.3. Creation of an Information Management Emergency Preparedness Plan and tool kit, as part of the corporate Emergency Response and Business Resumption Plan.
2. Physical controls may include:

- 2.1. Guidelines for facility environmental controls related to physical records storage, are implemented and storage area site audit visits are conducted at least twice a year.
  - 2.2. Provision of lockable cabinets, lockable storage rooms, and keys for secure access to records in business units.
  - 2.3. The regular promotion of clear desk practices.
  - 2.4. Making a back up copy of single source key hardcopy documents, either a scanned imaged, microfilm image, or photocopy produced and stored in an alternate location.
3. Technical controls may include:
    - 3.1. Standards or guidelines developed by Information Technology Services that align with this policy.
    - 3.2. Network and mobile device sign-ons that include passwords, with a requirement to change passwords at predetermined intervals.
    - 3.3. The use of firewalls, antivirus, and security software on all network and mobile devices.
    - 3.4. The requirement that all personal devices used to complete College business meet all College information technology standards, as well as all College information management standards.
  4. Red Deer College creates detailed standards for the Records and Information Management Program and publishes them in an online Records and Information Management Program Manual.

## **PROCEDURES:**

Below are five high level procedures that are explained in greater detail in their respective companion Standards in the Records and Information Management Program Manual.

### **1. Records Creation and Receipt**

- 1.1. Staff Members create a record when something they do provides a service, or is evidence of fulfilling a College obligation.
- 1.2. When creating or receiving a record, Staff Members are responsible for making sure the record is reliable, accurate and complete.
  - A record is *reliable* when you know and trust its source(s) of creation and you create and maintain the record in a way that protects it from unauthorized alteration, access or duplication.
  - An *accurate* record is one that a knowledgeable Staff Member can review for accuracy and that has information the creator can verify as true. Facts must not be misrepresented.
  - A record is *complete* if it reflects its purpose as outlined in the documented business process.
- 1.3. Staff Members must immediately advise their Supervisor/Manager when they discover any irregularities in records by making a report to the Supervisor/Manager and the Manager of Information Management.
- 1.4. When possible, Staff Members collect personal information directly from the individual and collect only the information needed to provide the service or complete the process. If necessary, Staff Members can also collect personal information

about an individual indirectly, through a third party (for example, to facilitate an investigation).

## **2. Records Use and Distribution**

- 2.1. The records that are created and received by the College are used within approved College systems for records management and are distributed in such a way as to ensure confidentiality and privacy are maintained. College records are only used for the purpose they were created, particularly when the record includes personal information capture, and that all reasonable steps are to be taken to ensure records are distributed through approved methods and only to approved recipients.
- 2.2. One of the College's Records Management goals is to avoid information duplication. The first step in accomplishing this is to identify multiple copies of the same record or document through the Records Inventory and another step is the use of document links as a means of distribution (instead of attaching documents).
- 2.3. Upon implementation, standardized, documented and approved systems are to be used to distribute (and track the distribution of) records and information internally and externally (for example sent by email, hardcopy mail, and faxes).

## **3. Records Storage, Protection and Security**

- 3.1. Records are stored in such a fashion as to facilitate retrieval, protection and distribution. The Records Taxonomy is used to organize both hard copy and electronic Records. The Taxonomy must be noted on the inventory when sending inactive hard copy records to inactive storage locations.
- 3.2. When appropriate, one or more of the following types of security controls is used to protect the College's Records: administrative controls, physical controls or technological controls.
- 3.3. All staff must maintain the security and confidentiality of College Records that are in their custody and the Records for which they are responsible. Records security and confidentiality must be maintained regardless of the Record's format, media or storage location.

## **4. Records Inventory**

- 4.1. Each record in the inventory is matched up with its counterpart retention rule and associated taxonomy code. This allows staff to easily link their department's inventory to the unique retention rules they are mapped to.
- 4.2. Staff Members update the Records Inventory when new record types are added to the business area's record collection. The update is sent to the business unit's Records Liaison who forwards the update to the Records Management team. The Record Management's team updates the corporate inventory.

## **5. Records Retention and Disposition**

- 5.1. The retention and disposition (destruction, deletion, indefinite retention) of College Records follow the Records Taxonomy, Retention and Disposition Schedule.
- 5.2. Staff Members maintain and dispose of Records that are in their custody or under their control. Records must be disposed of promptly upon the expiration of their applicable retention period. Any Records and Transitory Records on Litigation Hold are exceptions to Disposition activities and must not be disposed of until the release of all Litigation Holds for which the records are being held.

- 5.3. The Retention and Disposition Schedule and the Records Taxonomy apply to Records that were created or received after July 1, 2014. The application of the Schedule to legacy Records created or received prior to July 1, 2014 is that the Records are disposed of based on the College's Retention Schedule Implementation Plan.
- 5.4. Any extensions to the retention of Records and Transitory Records, beyond the periods specified in the Schedule, must be approved in writing by the Chief Information Officer.
- 5.5. Contracts and agreements stipulating that the College retain certain Records longer than retention periods in the Schedule, supersede the retention periods of the Schedule.
- 5.6. Inadvertent destruction of Records is documented by Staff Members and submitted to the Chief Information Officer.

**OFFICER RESPONSIBLE:** Vice President, College Services

**RECOMMENDING AUTHORITY:** Service Council

**CONSULTATION FOR REVIEW:** Campus Management, Deans' Council, Service Council, Finance, Human Resources, IT Services, Registrar

**POLICY REVIEW DATE:** July 2018

**EFFECTIVE DATE:** July 1, 2015

**REVISION HISTORY:** February 1, 2001 (Records and Information Management Standard Practice)  
August, 2004  
July 1, 2015 (revised and renamed Records and Information Management Policy)

**RELATED POLICIES:**

- Access to Student Academic Records
- Emergency Response and Business Resumption
- Information Assets and Information Systems Acceptable Use
- Freedom of Information and Protection of Privacy
- Web Site Privacy
- Information Requests – Formal Access Standard Practice

**CONNECTION TO BOARD POLICIES:**

All RDC policies support relevant Board of Governors policies.