Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Information Management
NO.:	ADMIN-242
RESPONSIBILITY:	Chief Administrative Officer
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	November 2023
REVISED DATE(S):	February 2024
REVIEW DATE:	November 2026

1. Introduction

Information governance encompasses records management, where “records” are the recorded information made or received by the College in the course of its administrative activities and kept as evidence of those activities.

2. Purpose

This policy and procedure establish a framework for the management of college information according to fiscal, legal and statutory requirements, archival value and administrative or operational needs.

3. Definitions

Refer to Durham College’s Standard Definitions.

4. Policy statements

This policy is designed to provide for the efficient and effective management of the College's information.

4.1. Scope

4.1.1. This policy and procedure apply to all information within the custody and control of the College and applies to the lifecycle of a record, from creation to disposition.

4.1.2. The College’s information exists in many formats, including electronic and hard copy textual documents, structured data, graphic images, sound and video recordings, or a combination of these formats. This policy and procedure addresses the management of all formats and the conversion of information from one format to another.

4.1.3. This policy and procedure apply to all individuals who create, use, manage and dispose of college information.

4.1.4. This policy and its procedures do not apply to:

a) Research and study notes, reports, manuscripts, publications, and personal communications of individual employees and students (unless specifically commissioned or prepared under contract for the College or prepared in the context of administrative work); or

b) Information placed in the College archives by or on behalf of a person or organization other than the College.

4.2. Basic principles

The following principles are based on the ARMA International Generally Accepted Recordkeeping Principles®

4.2.1. Principle of Accountability

- The College has appointed the Chief Administrative Officer to oversee the Information Management program and delegate responsibility for records and information management to appropriate individuals.
- The College will maintain a Common Records Retention Schedule (CRRS) to classify all information by the function and activities in which it is used, including documenting the Office of Primary Responsibility for the different classifications of information, the required retention periods for the information, and the final disposition (destruction, or long-term archival preservation).
- The College will promote orderly and efficient creation, use, maintenance, retention and disposition of information, and provide for information to be retained and preserved or destroyed according to fiscal, legal and statutory requirements, archival value and administrative or operational needs.

4.2.2. Principle of Transparency

- The College’s business processes and activities will be documented in an open and verifiable manner and the documentation will be available to all employees and appropriate interested parties.
- The College will provide for the preservation of information, which documents its activities and history. Information that documents the College’s history is generally classified as permanent in the Common Records Retention Schedule.

4.2.3. Principle of Integrity

- The College's information management policies, procedures, and standards will ensure the information generated by or managed for the organization is authentic and reliable.

4.2.4. Principle of Protection

- The College's information management policies, procedures, and standards ensure the protection of information that is personal, private, confidential, essential to business continuity, or otherwise requires protection consistent with fiscal, legal and statutory requirements.
- The College will establish and maintain information management policies, procedures, and standards for the secure and appropriate sharing of confidential information within the College, and when necessary with government and other agencies authorized to access and use that information.
- The College will establish a Privacy Breach Protocol to respond to incidents where personal information has been collected, used or disclosed in an unauthorized manner, or where a data breach has occurred.

4.2.5. Principle of Compliance

- The College's information management policies, procedures, and standards will be written to comply with fiscal, legal and statutory requirements, and generally accepted information management standards and best practices
- The College will provide training and resources to employees in order to meet their information management responsibilities and to achieve improvements in compliance, security, and risk management throughout the College.

4.2.6. Principle of Availability

- The College will maintain information in a manner that ensures timely, efficient, and accurate retrieval of needed information.

4.2.7. Principle of Retention

- The College will retain information according to the Common Records Retention Schedule, taking into account legal, regulatory, fiscal, and operational requirements and historical value.

4.2.8. Principle of Disposition

- The College will provide secure and appropriate disposition for information that is no longer required to be retained according to fiscal, legal and statutory requirements, historical value and administrative or operational needs.

5. Procedure

The following instructions will assist departments in managing their information throughout the information lifecycle according to ARMA's Generally Accepted Recordkeeping Principles®.

5.1. Initial Phase

5.1.1. Information created or received for business or operational needs shall be saved using the department's standard naming conventions and classified according to the Common Records Retention Schedule.

More information regarding standard naming conventions for information is available on ICE: https://ice.durhamcollege.ca/Admin/RM/Pages/Training.aspx

More information and training regarding the Durham College Common Records Retention Schedule is available on ICE: https://ice.durhamCollege.ca/Admin/RM/Pages/Schedule.aspx

To access the Durham College Common Records Search Tool: https://ssbp.mycampus.ca/apex/f?p=460:50

5.2. Active Phase

5.2.1. All active records will be retained within the department's central records. The following are accepted information storage areas:

- Electronic Records:
  - Official records must be stored on a shared network drive under department folders, and/or Banner.
  - Transitory records must be stored on your personal H drive, a network drive or OneDrive. Sharing and collaboration of transitory records is best done by using OneDrive. A laptop hard drive, external hard drive or USB key is not an official storage location.
  - Third-party software solutions that store College records used to conduct College business, must abide by our CRRS.

- Electronic Email/Chat Communication Records:
    - Official Email/Chat Communication containing an official record, whether the record resides in the email/chat application or as an attachment, must be saved in a retrievable format such as .msg or .pdf on a shared network drive under department folders, and/or Banner as per the Durham College Common Records Retention Schedule.
    - Electronic communication defined as "transitory email/chat communication" must remain within the College's official email application and/or approved chat/messaging applications.

- Physical Records:
    - Locked filing cabinets in the department's central filing area and/or
    - Locked filing cabinets within personal offices within the department.

NOTE**:** Any records containing personal information or personal health information must be stored in a locked filing cabinet behind a locked door.

5.2.2. Physical College records are to be inventoried as part of the Office of Primary Responsibility Records Inventory by the individual delegated with access to the Records Inventory Database and responsible for updating the department's records inventory.

5.2.3. Departments that retain a physical copy of the information are also required to inventory the record as part of their department's records inventory using the Records Inventory Database, indicating where required on the entry form that the information is a copy.

More information and training regarding the Records Inventory Database is available on ICE:

https://ice.durhamCollege.ca/Admin/RM/Pages/Records-Inventory-Database.aspx

To access the Records Inventory Database:

https://ssbp.mycampus.ca/prod/f?p=460:101:1739898388399

To add a user for your department, please contact the Office of Records Management at ext. 3139 or DCrecordsmanagement@durhamcollege.ca.

5.3. Inactive Phase

5.3.1. Inactive electronic records including official email/chat communication records are to be stored as part of the Office of Primary Responsibility's central electronic records for the remainder of the required retention period as per the Common Records Retention Schedule.

5.3.2. All electronic records including official and transitory email/chat communication records are deemed inactive upon the exit of an employee from the College. To support business continuity, a supervisor must request temporary access to the employee’s MS365 account and any other systems within 30 days of the employees exit.

5.3.3 To allow Durham College to retrieve any official records from a former employee, the supervisor or their designate must complete the retrieval and saving of active records of value, based on the Common Records Retention Schedule within 6 months of an employee’s exit. This temporary access is automatically disabled on the 181st day.

5.3.4. All electronic records including email/chat communication records will be permanently deleted 24 months from the date of exit unless an Information Hold has been applied. Electronic records including email/chat communication with an Information Hold will be retained until the hold has been resolved.

5.3.5. All electronic records including email/chat communication created by an Executive Leader will be retained for 51 years upon their exit from the College.

5.3.6. Inactive information in a physical format may be transferred to the Central Inactive Records storage area if departments do not have adequate space to store the information for the entire retention period. Please refer to the Durham College Common Records Retention Schedule for the required retention period within the department’s office space.

5.3.7. As per the Common Records Retention Schedule, when a physical record is no longer deemed active it should be processed and moved to inactive storage. To transfer records, the Records Management Liaison for the department must complete a Records Transfer Form and submit it to the Records Manager.

More information regarding the Records Transfer process and the Records Transfer Form is available on ICE: https://ice.durhamCollege.ca/Admin/RM/Pages/Records-transfer-destruction.aspx

5.4. Disposition Phase

5.4.1. Information will be disposed of according to the disposition indicated for the classification in the Common Records Retention Schedule except for transitory email communication.

5.4.2. All email/chat communication records will be deleted by IT Services as part of their account management services 24 months from the official exit date, as provided by Human Resources, of an employee from the College. When an employee's Email/Chat Records are deleted the employee's complete Microsoft 365 account and the employee's home drive (H-drive) will also be deleted.

5.4.3. The Records Manager will provide each department's Records Management Liaison with an annual report generated from the Records Inventory Database detailing the information within their department's inventory that is past the required retention period.

NOTE: This report can only be provided if the department has utilized the Durham College Records Inventory Database.

5.4.4. Secure Destruction

Records containing sensitive or confidential information or personal information require secure destruction. Secure destruction maintains security throughout the destruction process and renders the Record unrecoverable. Secure destruction services may be contracted from third-party service providers.

- The Records Manager Liaison and the Records Manager will complete the required Destruction Form for approval by the department's Manager, and the Executive Dean/Dean or Vice-President for the department.
- A designated person must witness the secure destruction of the eligible records or the removal of eligible records for destruction by a third-party service provider.
- The Records Manager will add a record of the destruction date to the Durham College Records Inventory Database.

  More information regarding the Records Destruction process and the Records Destruction Form is available on ICE:

  https://ice.durhamCollege.ca/Admin/RM/Pages/Records-transfer-destruction.aspx

5.4.5. Campus Library Archives

College Records to be reviewed for historical value will be identified in the Common Records Retention Schedule. The Retention will be permanent or the disposition will require archives review prior to destruction.

- The Records Management Liaison will contact the Records Manager to request a review of the information for historical value, according to the retention or disposition indicated for the classification in the Common Records Retention Schedule. The Records Manager will review the information with the Campus Library Archives Technician and Chief Librarian to determine if the information is of historical value.

- If the information is deemed to have historical value, the information will be transferred to the Campus Library Archives for permanent storage. The Records Manager will work with the department to facilitate the transfer process.

- The Records Manager will coordinate the transfer of records identified for annual transfer to the Campus Library Archives with administrative staff and the Chief Librarian.

- Durham College institutional records stored in the Campus Library Archives are controlled and access to them is only with permission of the Chief Librarian. Generally, these restricted records are made available to members of the Durham College Board of Governors, the President, the Chair of the administrative committee or the head of the business unit responsible for the administrative committee, and authorized Durham College employees requiring access to fulfill his/her responsibilities. Notification of authorization for these delegated persons to access the institutional records must be forwarded to the Chief Librarian. Once authorization has been received, access to the records identified in the authorization will be given.

- External requests for access to the Durham College's current and non-current historical institutional records should be made through the Durham College Freedom of Information and Protection of Privacy Coordinator. A written application is required citing records required, the purpose of the research, and giving commitment to confidentiality. Once the application is approved by the Freedom of Information and Protection of Privacy Coordinator and given to the Chief Librarian, individuals will have access to the records outlined in the approval.

5.5. Information Hold

5.5.1. The Records Manager will issue a written Records Hold notice when:

- there is a potential legal dispute, litigation or other legal matter
- there is an operational or audit need for Records
- requested by the Freedom of Information and Protection of Privacy Coordinator

5.5.2. The Records Hold notice will identify the affected Records Classification and an anticipated end date for the Records Hold.

5.5.3. Copies of Record Hold notices will be sent to:

- President;
- Vice-Presidents;
- Associate Vice-President, Information Technology;
- Freedom of Information and Protection of Privacy Coordinator;
- Responsible Departments (Office(s) of Primary Responsibility for Records Classification);
- System Administrators of involved systems; and
- any other necessary employees

5.5.4. Upon being notified of an Information Hold, the responsible units will suspend all disposition of affected Information immediately. Information Holds will remain in effect until rescinded in writing by the Records Manager.

5.5.5. Records Classifications requiring repeated operational or audit Record Holds will be evaluated by the Records Manager to determine if their Retention Period continues to meet Durham College's operational needs, or if a revision is required.

5.6. Revisions to the Common Records Retention Schedule

5.6.1. Requests for changes to the Common Records Retention Schedule shall be submitted to the Records Manager. Changes may be required for the following reasons:

- Changes to legislation or regulations that will affect recordkeeping;
- New guidance from professional or accreditation bodies that will affect recordkeeping;
- Changes to information systems used in recordkeeping; or
- Changes to responsibility for recordkeeping (new programs, transfer of responsibility between departments, etc.)

5.6.2. For any requested changes to the Common Records Retention Schedule, the following information is required:

- Records Classification requiring revision; and
- Nature of the revision, such as change to the retention period, Office of Primary Responsibility, Retention Rationale (legislative requirements etc.)

5.6.3. The Common Records Retention Schedule will be evaluated along with all Information Management policies and procedures every three years.

This evaluation by the Records Manager will determine if revisions are required for existing classifications or if new classifications are required.

5.6.4. Any revisions to the Common Records Retention Schedule will be presented to the Durham College Leadership Team for approval.

5.7. Information Management Audit

- The Records Manager will work with the Records Management Liaison to conduct an Information Management audit of each department every three years. This audit will evaluate compliance with key components of the Information Management policy and procedure.

- The audit checklists and remediation plan for each department/academic school will be signed by the department manager/executive dean/dean. A full audit report will be presented to the Durham College Leadership Team.

6. Roles and responsibilities

6.1. The Durham College Leadership Team is responsible for reviewing and approving the policies, procedures, and other controls required for security, lifecycle management, risk management, and quality assurance of College information.

6.2. The Chief Administrative Officer is responsible for overseeing the Information Management Program and delegating responsibility for Information Management to the appropriate individuals.

6.3. The Records Manager is responsible for developing and recommending to the Chief Administrative Officer and AVP, Information Technology policies, procedures, standards and guidelines and other controls for information lifecycle management, risk management, quality assurance, appropriate use and security of information.

6.4. The AVP, Information Technology, Freedom of Information and Protection of Privacy Coordinator and Records Manager are responsible for implementing and maintaining the security controls that enforce the rules and procedures for Information Management.

6.5. The individual in the most senior position in each department is responsible for identifying the Records Management Liaison in their department and delegating responsibility for implementing Information Management policies, procedures, standards and guidelines within their department.

6.6. The department Records Management Liaison will be the key contact within their department for the Records Manager. They will receive updates regarding changes to the Common Records Retention Schedule, Information Management policies, procedures, standards and guidelines, and implementation. The

Records Management Liaison will attend training and information sessions, and share information with all employees in their department.

7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure and it adheres to the principles outlined in the College's commitment to accessibility as demonstrated by the Multi-Year Accessibility Plan.

8. Non-compliance implications

Non-compliance could affect the College's ability to conduct business, respond to requests for information, be transparent and accountable, and ensure confidentiality and privacy of personal information. This would be a risk to the College both financially and to our reputation in the community.

9. Related forms, legislation or external resources

- Records Transfer Form
- Records Destruction Form
- FIPPA and Its Application to Durham College