INFORMATION AND RECORDS MANAGEMENT POLICY
OF THE
ALMA MATER SOCIETY
OF QUEEN'S UNIVERSITY

Responsibility	Information Management Specialist
Approved by	Board of Directors
Date initially approved	July 9, 2017
Date last revised	October 29, 2025

Table of Contents

Land Acknowledgement

We acknowledge that we are on the traditional lands of the Anishinaabe and Haudenosaunee peoples, known as Katarokwi, or colonially as “Kingston.” The Alma Mater Society at Queen’s University seeks to recognize the importance of these lands to the Indigenous peoples who have existed since time immemorial. The unjust acquisition of these lands occurred through the Crawford Purchase of 1783, a land treaty upheld by the First Peoples but later undermined by the British Crown and the “Canadian” government. This history of numerous broken promises and treaties continues to impact Indigenous communities today.

As settlers on this land, we acknowledge our continued benefit from systemic structures that marginalize Indigenous peoples. Recognizing systemic oppression, it is our duty to actively listen to and amplify Indigenous voices, addressing both past and ongoing injustices for meaningful, positive change. We are grateful to these lands for sustaining us and giving us the gift of life. This acknowledgment is a call to action, committing us to understand and respect the history and ongoing struggles of Indigenous peoples. We recognize that words alone are not enough; our actions must reflect our commitment to justice and reconciliation.

Purpose

The purpose of this policy is to provide direction regarding the creation, storage and management of information and records at the Alma Mater Society of Queen’s University Incorporated (AMS). The policy will clarify responsibilities for all AMS staff with regards to protection of personal and corporate information, reduction of risk regarding loss or exposure of information, and access to information.

Policy Statement

AMS Information Assets are vital for ongoing operations and for records of business decisions, activities, and transactions. Information Assets are crucial for ensuring a smooth transition between outgoing and incoming AMS administrations. All Information Assets created for AMS business or activities are the intellectual property of the AMS and may not be retained by AMS staff. The AMS is committed to:

- Establishing and maintaining information and records management practices that meet the business needs, accountability, and archival recordkeeping requirements of a private non-profit corporation and the expectations of its stakeholders
- Protecting personal information by responsibly managing and disposing of the information in a secure manner
- Implementing customized information and records management policies, practices, procedures, and systems to ensure the creation, maintenance, and protection of Information Assets
- Providing a reliable and accurate record of current and historical business decisions and actions taken by the AMS to support the organization and students at large

All information and records management practices at the AMS are to be in accordance with this policy and its resulting procedures.

Scope

This policy applies to all AMS Staff including executives, officers, directors, commissioners, employees, and volunteers, as well as permanent staff and contractors. All Information Assets created by these individuals are Information Assets and the intellectual property of the AMS.

This policy covers all information and records in all digital formats and on paper.

Terminology

Archive(s): Repository of Information Assets that were created in previous years and have been retained based on the business and/or historical value of the information contained in the documents.

Archival value: information that has been deemed to have historical significance for the AMS by the Information Management Specialist.

Business value: any information that has been deemed by the Information Management Specialist as important for ongoing reference or proof of the operational and/or administrative decisions and/or actions of the AMS.

Disposition: a final decision regarding the value of information and if the information will be permanently archived or destroyed.

Document(s): a container of information. This includes all text, graphics, photos, video, and audio in all digital and physical formats. This term may be used interchangeably with the term “file” or “paper record”.

Information: the content of a document.

Information asset: any document in any format that has been created and saved in any AMS Repository.

Microsoft 365 (M365): the suite of online or cloud applications used by the AMS. This includes Teams, OneDrive, Outlook, Calendar, OneNote, etc. It also includes all productivity tools including Word, Excel, and PowerPoint. (Microsoft 365 formerly known as Office 365).

Must: a word to indicate that a section or clause of this policy is mandatory and must be followed.

Office: a commission, service, or office of a director or an executive.

Owner: the individual who created information and has care and control of the document.

Personal information: any information (demographic, contact, government, or institutional identification numbers) about an individual that may be used to identify an individual.

Personal device(s): any personally owned desktop, laptop, tablet, mobile phone and/or portable storage device of any kind.

Public: individuals or groups who are not AMS employees or volunteers, including students at large, university partners, member societies, the Kingston community, and the public.

Record: a document of business and/or archival value that is accepted as genuine and accurate.

Repository: any storage facility, physical or virtual, on premises or off that is used to retain AMS Information Assets and records.

Restricted information: any information that is considered by the owner or the AMS to be private, privileged, sensitive, confidential, or strategic.

Retention: the period that a document is kept in an AMS information Repository for the use of the AMS.

Retention and disposition guide: a list of files that have been created and saved by owners and has been assigned a retention period or destruction label by the Information Management Specialist.

Should: a word to indicate that a section or clause of this policy is recommended but not mandatory.

Staff: all student and permanent staff employees, as well as any volunteers and contractors with access to AMS Information Assets and Repositories.

Third-party vendor: an organization outside of the AMS that is providing a service related to communications and/or information management.

Transitory: information that is a draft, incomplete document, third-party research and/or minor version of a document, that is found to be redundant, obsolete and/or trivial by the Information Management Specialist, and that has been deemed to not have “archival value” or “business value”.

Roles and Responsibilities

- **All volunteers, contractors, student, and permanent staff** have the responsibility to comply with this policy and to seek assistance from the Information Management Specialist if need be.

- **Executive members, IT officer and The General Manager** will require compliance with this policy and ensure that the AMS information and records management program is adequately resourced.
- **All executives, commissioners, directors, and managers** are responsible for receiving and understanding training delivered by the Information Management Specialist and/or seeking assistance from the Information Management Specialist. Named individuals holding

these positions are also responsible for supporting and promoting this policy within their respective offices. Any barriers to compliance with this policy must be reported to the Information Management Specialist.

- **The Information Management Specialist** is responsible for helping users and determining the business and/or archival value of Information Assets, and for overseeing the management of information and records of all executives and staff under one-year employment contracts at the AMS.

- **The vice-chair of the AMS Board of Directors** is responsible for overseeing the management of information and records of the AMS Board of Directors.

- **The executive and general manager** are responsible for overseeing the management of all financial information and records for all executive offices, commissions, services, and general office administration.

- **The human resources officer** is responsible for all student employee information and records with the advice and assistance of the Information Management Specialist regarding retention periods and disposition.

- **The general manager** is responsible for all permanent staff employee information and records.

- **The information technology** officer is responsible for maintaining information technology resources for AMS information and records systems, including maintaining appropriate system accessibility, security and back up.

- **Any contract staff** hired by AMS managers must not retain, in any way, information and/or records produced while under contract with the AMS. The AMS executive must require that AMS Information Assets produced by contract staff are stored in compliance with this policy.

Policy

1. Recordkeeping and privacy requirements

a. As a not-for-profit corporation, the AMS must maintain records of finances (audited financial statements), agendas and minutes of membership (Assembly and Board) meetings.

b. Retention of financial records and human resources records must be retained according to specific and applicable legislative requirements.

c. Membership lists containing personal information must be securely deleted and/or destroyed after use by the AMS office that collected and/or has been given access to the information.

2. Creating, saving, storing, and managing documents

a) The only Repository for AMS information and records is the AMS Microsoft 365 (M365) online Repository. Microsoft 365 data is backed up 3 times daily in a Canadian Cloud storage location for business-critical restorations.

b) All documents must be stored in the appropriate folder, utilizing the folder structure, as directed by the Information Management Specialist.

c) All documents must be named according to the AMS File Naming Guide made available by the Information Management Specialist.

d) The unauthorized use of **personal or self-created** third-party vendor file storage, sharing and communication tools such as Google, Dropbox, etc. is **prohibited**.

e) We maintain a **Digital Ecosystem** that serves as a centralized inventory of all software and digital tools approved by the IT Steering Committee. This ecosystem provides a clear reference point for students, staff, and stakeholders by outlining which software solutions have been reviewed, approved, and deemed appropriate for use within AMS.
The Digital Ecosystem not only helps ensure consistency and security across our operations but also supports transparency by allowing users to identify which applications are officially supported. By consulting this resource, students can confidently determine which software is authorized for academic and organizational purposes, reducing risks associated with unverified or unsupported tools.

f) Authorized third-party vendor tools may be used for AMS business proposes and must be approved by the Information Technology Steering Committee (ITSC). Personal devices and/or hard drives of any kind must not be used to save and/or store AMS documents for any reason. The AMS is **NOT** responsible for personal data stored outside of approved ecosystems.

g) In limited circumstances, such as for particular security and/or privacy purposes, there may be a requirement for the printing and storage of documents. The Information Management Specialist is available for advice in these instances.

h) File owners may destroy and/or delete working or temporary documents that are considered transitory in nature. File owners should consult the Guideline for Transitory Documents or contact the Information Management Specialist for guidance.

i) Recordings of meetings may be saved by the meeting organizer within an appropriate area of M365. The Information Management Specialist should be consulted regarding the storage location. Recordings must be managed by the meeting organizer and follow the directives in this policy.

3. Access to Information Assets

3.1. Collaboration and/or off-site access

a. All AMS staff must use M365 tools for collaboration or web access and/or storage tool and/or any portable storage device is prohibited.

b. Collaboration with authorized external parties may be accomplished by using M365 tools with the appropriate security settings.

c. Access to documents saved on the AMS Repository is restricted to the owner, the information technology officer, and the Information Management Specialist. Other individuals may be authorized to have access by the executive and general manager and will be facilitated by the Information Management Specialist.

3.2. Use of personal devices to access information

a. Personal devices must **only** be used to access AMS Information Assets through M365 tools.

b. Personal devices used to access, create, or share AMS Information Assets must be password protected and further secured by at least one form of multi-factor authentication.

3.3. Transfer of files

a. AMS's Preferred file sharing methodology is to leverage Microsoft 365 Shared Links (OneDrive, Teams and SharePoint), however where longer file sharing continuity is required (because links do eventually time out or can be moved), sharing via email attachment is authorized, but not recommended.

b. AMS files should be password protected when emailed outside the AMS and **must** be password protected when personal information of any individual is included in the document. The Information Management Specialist is available for assistance.

c. Human Resources (HR) files are created, stored, and accessed using a third-party vendor (Citation Canada) for all HR related documentation. Older files (pre-2021-22) will be archived on the HR Teams site.

d. AMS files must not be transferred inside or outside the AMS by using external storage devices such as USBs or other portable hard drives regardless of the ownership of the device.

e. AMS files may be transferred within the AMS by using M365 tools.

f. AMS files may be transferred outside of the AMS by utilizing M365 tools with appropriate permission settings and after consultation with the Information Management Specialist.

g. File owners must consult with the Information Management Specialist regarding transfer of files for any other situations not covered by this policy

4. Personal information

a) Collection of any personal information for any purpose must be approved by the executive, in consultation with the Information Management Specialist and/or IT Officer.

b) Files that contain personal information must be password protected.

c) Files that contain personal information must be securely deleted and/or destroyed after the purpose of collection has been fulfilled or the specific retention period has expired.

d) Files that contain personal information must only be stored in the AMS M365 Repository in the appropriate location and in consultation with the Information Management Specialist.

e) Internal sharing of files that contain personal information must be approved by the executive and in consultation with the Information Management Specialist.

f) External sharing of personal information files must be in consultation with the Information Management Specialist, receive express written consent of the individual concerned, and of the AMS executive.

g) Personal information provided by the university registrar's office to the AMS president must remain confidential and it is the responsibility of the president to follow the directives of the annual information sharing agreement signed with the university. The Information Management Specialist must carry out and/or confirm the deletion of the information by the president annually as stipulated in the agreement.

5. Restrictions

a) Staff are restricted regarding information and records by the terms of the AMS Confidentiality and Non-Disclosure Agreement signed at the time of employment.

b) Student numbers must not be collected for providing services or organizing events, except for where the Information Management Specialist has been consulted, and authorization has been given by the executive.

c) Staff must not access folders and files that are not pertinent to the performance of their duties, should this information inadvertently be revealed.

d) Staff must not store any personal photo, video, audio, and/or text files within AMS M365 applications or on AMS computer hard drives.

e) Staff may not, under any circumstances, destroy and/or delete files that have been deemed to have business and/or archival value by the Information Management Specialist.

6. Public access to AMS information

a) The primary channel for providing corporate information to the public is the AMS website. The website is managed and updated by the Communications Office.

b) All social media accounts must be approved by the executive and content governed by Communications Office and the marketing officer.

c) Information and records published on the AMS website or approved social media channels must be approved by the executive and some cases the AMS Board of Directors.

d) Management of passwords for all communication channels is the joint responsibility of the director of communications, marketing officer, and the information technology officer, as determined from time to time.

e) Websites and social media accounts for services and programs must be approved by the executive.

f) Management of websites and social media accounts for services and programs are the responsibility of the executive.

7. Retention and disposition

7.1. Retention

a) Except for financial and human resources information, the Information Management Specialist shall appraise documents within the purview of the information office (IT, executive, and senior management of commissions, offices, and services) to identify documents of business and/or archival value. Appraisal will be carried out following a full three-year retention period. The Information Management Specialist will manage the permanent retention of identified Information Assets on AMS M365.

b) Retained Information Assets of business and/or archival value are records of the AMS and will be permanently retained in the Archives folder for each office and/or any other Archives Repository within AMS M365.

c) Retained and archived Information Assets shall be available to staff by accessing archives folders or requesting assistance from the Information Management Specialist.

7.2. Disposition

a) Information Assets that are appraised and are not identified for retention must be securely destroyed and/or deleted by the Information Management Specialist.

b) Digital Information Assets designated for deletion must be deleted on AMS M365.

7.3. Retention and disposition of legal hold records

a) Records that have been identified as necessary for legal proceedings or potential legal proceedings are in complete control of the general manager.

b) The general manager may securely retain legal hold records for an unlimited time.

c) Following consultations with AMS legal counsel, the general manager may decide to securely destroy and/or delete legal hold records.

8. Management of paper documents

a) Printing and filing of working (transitory) documents **must** be minimized.

b) Personal, restricted and/or confidential information, collected with the permission of the individual(s), should not be printed unless necessary. If printing is necessary, the security of the document(s) is the sole responsibility of the person who printed the document(s). The printed document(s) must be filed in a secure manner within the office of origin and must be destroyed in a secure manner and appropriate time frame when the purpose of printing has been fulfilled. Consult with the Information Management Specialist if there are any questions.

c) Paper documents containing personal information must be securely destroyed (shredded on premises) when the information is no longer needed for the intended purpose.

d) Document owners should consult the Information Management Specialist regarding the management of all paper records including the secure destruction of documents.

e) The Information Management Specialist shall offer paper document management advice, including appraisal, retention, and disposition, to all office staff before April 30 of each year.

f) Paper documents deemed by the Information Management Specialist to be of archival value to the AMS will be retained by the Information Management Specialist in as a paper record and/or scanned document for storage within M365.

g) Paper documents that are necessary for administrative and/or operational reasons that contain sensitive or confidential information will be retained in a secure manner in the office of origin.

h) Paper documents of offices that have been dissolved will be appraised by the Information Management Specialist for retention and/or disposition.

i) Paper documents of offices that are merged with newly created or existing offices will be appraised by the Information Management Specialist for retention and/or disposition and filed appropriately with M365.

9. Meeting recordings

a) Offices may retain meeting recordings within M365 in consultation with the Information Management Specialist.

b) The AMS leverages **AI-enabled meeting software "Meeting Insight"** to enhance productivity and accessibility. These tools may assist in generating **meeting notes**, including key discussion points, action items, and decision summaries. By using AI to provide structured meeting notes and summaries, participants can focus more fully on active engagement, while ensuring that accurate records are available for follow-up and accountability.
In addition, when a meeting is being recorded, the system will always issue a clear **"Meeting Recording" alert** to all attendees. This ensures that participants are fully informed whenever recording is in progress. Recordings are retained only for official purposes, such as documentation or compliance.

c) Recordings of meetings **must** not be considered as replacements for meeting written minutes or notes. Recordings must only be retained for reference until minutes are written and approved, at which time the recording **must** be deleted.

d) The Information Management Specialist may retain selected recordings of historical significance for inclusion in the Archives Repository within M365.

10. Transfer of archived records

a) Certain records that have been archived in paper and/or digital form may be designated to be offered to Queen's University Archives to ensure the long-term security and availability of the records.

b) The Information Management Specialist will periodically appraise and select archived records in preparation of a report that makes recommendations regarding the offer of records to Queen's University Archives.

c) Should Queen's Archives agree to receive the records, the final decision regarding transfer of the records will rest with the executive and the general manager.

d) Records refused by Queen's Archives will be appraised and be retained or deleted and/or destroyed by the with approval of the executive and the general manager.

11. Monitoring

a) Compliance with this policy will be monitored by the Information Management Specialist with the support of the executive and the general manager.

b) Regular policy review will be part of the monitoring process and changes to this policy will be integrated by the Information Management Specialist and submitted to the Board of Directors for approval.

Contact person	*Information Management Specialist*
Date of next review	*2027 - 2028*
Related policies, procedures and guidelines	*InfoTech Policy* *Board of Directors Policy Manual* *Personnel Records Policy*
Policies superseded by this policy	-