

8.

RECORDS AND INFORMATION MANAGEMENT

Overview

This chapter is intended to help public bodies understand how good records and information management practices assist in the effective administration of the *FOIP Act*.

All types of organizations, including public bodies, manage their recorded information for reasons that are significantly broader than compliance with access and privacy legislation: they create, maintain and manage records to provide tangible evidence of their business activities and transactions.

The primary purposes for records and information management are to

- support policy formation and managerial decision-making;
- improve client services and support better performance of business activities;
- support consistency, continuity and productivity in operations, administration and management;
- protect the interests of the organization and the rights of clients, the public and employees;
- provide protection and support in litigation, including the better management of risks associated with the existence or lack of evidence of activities or events;
- facilitate research and development activities; and
- enable organizations to meet legislative and regulatory requirements.

Also, to meet their obligations under the *FOIP Act*, public bodies need to have in place effective records and information management practices. Such practices should be modelled on national and international standards such as:

- International Standards Organization Records Management Standard (ISO 15489);
- Canadian General Standards Board standards for documentary evidence; and
- ARMA International's standards and guides (see www.arma.org).

8.1 Scope

Service Alberta administers the records management program in government. Alberta government departments, boards and agencies subject to the Records Management Regulation (AR 224/2001) must adhere to the policies and guidelines established under this Regulation.

For provincial government departments and their affiliated agencies, boards and commissions (FOIP Regulation **Schedule 1** public bodies), this chapter supplements the policies and guidelines issued by Service Alberta.

More detailed information on records and information management practices may be obtained from publications produced by Records and Information Management, Service Alberta (www.im.gov.ab.ca), such as:

- *Information Assets in the Government of Alberta: A Management Framework*
- *Information Management Planning*
- *Information Security Classification*
- *Official and Transitory Records: A Guide for Government of Alberta Employees*
- *Developing Records Retention and Disposition Schedules*
- *Managing Electronic Mail in the Government of Alberta*
- *Managing Instant Messages in the Government of Alberta*

Local public bodies are not subject to the provincial Records Management Regulation. Under **section 3(e)(ii)** of the *FOIP Act*, regulation of records management in local public bodies must be by bylaw, resolution or other legal instrument by which a local public body acts, or, in the absence of such a legal instrument, as authorized by the governing body of the local public body.

Records scheduling and disposition in local public bodies should be based on recognition of the role of records management in effective public administration. In particular, local public bodies should be aware of the importance of an authorization process for the disposition of records that ensures that the local public body can meet its financial and legal obligations, including its obligations under the *FOIP Act*.

8.2 Powers of the Commissioner

Section 53(1)(a) of the Act authorizes the Information and Privacy Commissioner to monitor the general administration of the *FOIP Act* to ensure that its purposes are achieved. This includes conducting investigations to ensure compliance with rules relating to the destruction of records set out in

- any other enactment of Alberta;
- a bylaw, resolution or other legal instrument by which a local public body acts; or
- any rules relating to the destruction of records that are authorized by the governing body of a local public body.

Public bodies, therefore, should expect their records and information management practices to be under scrutiny during reviews, investigations and privacy audits conducted by the Commissioner's Office. This is especially the case when an applicant requests a review of the adequacy of a search for information or records.

8.3 Records and Information Management Principles

The following principles underpin the effective management of recorded information.

Information is an important asset of the organization

An essential principle for the management of recorded information is that information is managed as a resource or asset of the whole organization and not as the property of individuals, branches or divisions.

The management of information is planned

An organization's business planning processes require both strategic and operational records and information management planning.

A life-cycle management approach is adopted

Sound principles for the management of recorded information are based on the life cycle of information. Management activities within the life cycle encompass

- the planning of information systems, including appropriate controls over the collection, creation or compilation of recorded information;
- the establishment of practices and procedures governing the organization, distribution, retrieval, use, accessibility, and transmission of the recorded information and for its storage, maintenance and protection;
- provision for routine disclosure and dissemination of such information, as appropriate; and
- the regulation of the scheduling and disposition of all recorded information.

All records are included

Management practices should apply to all records as defined in the *FOIP Act*, including personal information and electronic records.

Electronic records include

- electronic documents, such as word processed documents, e-mail, web pages, graphics, digital photographs, and scanned images; and
- electronic data, such as information stored in databases.

Electronic records include information in all media and in all locations. For example, electronic records may be stored on networks, local hard drives, portable hard drives, and personal digital assistants, as well as in portable storage devices, such as CDs, USB drives, DVDs, and tapes.

Accountability is assigned

In the case of provincial government departments and FOIP Regulation **Schedule 1** public bodies, the Records Management Regulation assigns accountability for records management in the public body to the deputy head.

Given the close relationship between the *FOIP Act* and the effective management of recorded information, there should be a similar assignment of accountability for the management of recorded information in local public bodies.

**8.4
Records and
Information
Management
Policy
Components**



Policies and guidelines should govern the management of recorded information in a public body.

Policies and guidelines should be developed with the administration of the *FOIP Act* in mind and should include appropriate references to access to information and protection of privacy requirements in policy statements, procedures, practices and standards.

The following components should be included in policies and guidelines for the management of recorded information:

- life-cycle management of recorded information;
- establishment and maintenance of a records system;
- a guide to personal information banks;
- guidelines for the creation and generation of records;
- a guide for transitory records;
- records management in contracting;
- scheduling and disposition of recorded information;
- guidelines and practices relating to the retention and disposition of e-mail and other forms of electronic messages;
- rules for the organization, storage and protection of recorded information;
- rules for the organization and management of electronic records;
- records system requirements for planning and designing electronic applications that will collect, create or generate information used by the public body; and
- security.

Managing recorded information throughout its life cycle

A public body should plan, direct, organize and control recorded information throughout its life cycle, regardless of the form or medium in which the information is held.

Establishing and maintaining a records system

A records system, which may be computerized or manual, is an information system that captures, maintains, manages and provides access to records over time. Increasingly, organizations are implementing specialized electronic records and document management technologies to support this function.

A records system should be controlled by a current and comprehensive classification structure, to arrange, locate and retrieve recorded information in the custody or under the control of the public body. The classification structure should link to the organization's records retention and disposition schedules to facilitate effective disposition practices. For provincial government departments and FOIP Regulation **Schedule 1** public bodies, the *Administrative Records Disposition Authority (ARDA)*

and the *Transitory Records Retention and Disposition Schedule*, published by Records and Information Management, Service Alberta, are generally used for the disposition of administrative and transitory records respectively.

The records system should serve as a locator system for all holdings of recorded information. It should also identify the business unit responsible for particular information holdings. In addition, it should support the application of privacy protection measures and support vital records identification for business resumption planning purposes.

Establishing and maintaining a directory of personal information banks

Section 87.1(1) requires the head of a public body to publish a directory, in printed or electronic form, listing the public body's personal information banks (PIBs). This applies to government departments and **Schedule 1** public bodies, as well as to local public bodies. For government departments and **Schedule 1** public bodies, personal information banks are identified in records schedules. **Section 87.1(2)** sets out the elements that must be included in the directory for each PIB.

For more information on PIBs, see *Guide to Identifying Personal Information Banks*, published by Access and Privacy, Service Alberta.

For more information on directories of records, see section 2.7 of Chapter 2.

Creating, maintaining and using records

Effective controls over the creation, maintenance and use of recorded information in the conduct of the business of the organization should be established through a written guideline.

The guideline should indicate what records need to be created and maintained. For example, records required for legal, fiscal, audit, administrative or operational purposes should be retained in a records system. For a discussion of what records should be created, which records should be retained and filed, and which records can be routinely destroyed within the Government of Alberta, see *Official and Transitory Records: A Guide for Government of Alberta Employees*, published by Records and Information Management, Service Alberta.

Any established guideline should be understood and followed by all public body officials and employees.

Scheduling and disposing of recorded information

Control over the disposition of recorded information is an important aspect of records and information management that is critical to FOIP administration. When responding to a FOIP request, it is necessary to know whether records have been destroyed and if so, whether this has been done in an authorized manner.

It is equally important to dispose of personal information under conditions that protect the privacy rights of the individual. Records retention and disposition schedules are a public body's legal authorities on how long recorded information

must be kept and how it is to be disposed of, e.g. by destruction or archival preservation.



Each public body should establish a scheduling process that governs the retention and final disposition of all the recorded information in its custody or under its control.

For public bodies subject to the Records Management Regulation, the Alberta Records Management Committee approves records retention and disposition schedules. The schedules provide authority to transfer inactive records to off-site storage, for destruction of records, and for the transfer of records selected for archival preservation to the Provincial Archives of Alberta. See also the Government of Alberta's Transitory Records Schedule under the Records Management Regulation.

The scheduling process and guidelines for the transfer and destruction of records are discussed in *Developing Records Retention and Disposition Schedules*, published by Records and Information Management, Service Alberta, and in related Alberta Records Management Committee Circulars.

Securely disposing of personal information

Authorized disposition of personal information may occur through

- transfer of records to the custody of the Provincial Archives of Alberta or the archives of a public body;
- physical destruction of records containing personal information in such a way that it cannot be retrieved or reconstructed; or
- alienation of records as a result of a privatization arrangement or the transfer of service delivery to another body. This disclosure must be authorized by law (a public body that is subject to the Records Management Regulation must have a Records Alienation Schedule approved by the Alberta Records Management Committee to authorize the transfer of records to a non-provincial government organization).

For other public bodies, authority to approve the transfer or destruction of the public body's recorded information will come from its governing body. A public body may have its own archives, or may select the archives of another public body or another archival facility to act for it.

Public bodies must pay strict attention to disposition processes for records. This is true for all recorded information, but particularly so for personal information. Disposal and preservation should be governed by well-documented and well-understood procedures. Commercial pulping or shredding is the best way of disposing of paper and other hard copy media. This should be done using equipment or in a facility that can ensure complete and secure destruction.

All too often, sensitive personal information intended for destruction is left in unsecured conditions and may be exposed to unauthorized access and, possibly, use. Examples include disposal of documents containing personal information in garbage

bags that have ripped open and disposal of personal information in a recycling container.

In *IPC Investigation Report 99-IR-003*, it was noted that the method of recycling that had been used was inappropriate since it exposed employees of the public body and citizens to the risk of misuse of their personal information.

Securely disposing of electronic records

Used office and computer equipment poses a special risk. In one investigation by the Information and Privacy Commissioner, filing cabinets were found to have been moved to an auction centre with files containing personal information still inside. Computer hard drives have been similarly put up for auction with information still stored on them.

At a minimum, computer hard drives need to be professionally wiped clean of data before they are disposed of or sold. See *Security Policy for Disk Wiping Surplus Computers*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

Provincial government departments and FOIP Regulation Schedule 1 public bodies are required



- to have operable hard drives wiped of all data by the ministry in accordance with specified procedures prior to sending the computers to Surplus Sales in Service Alberta; and
- to remove and destroy the hard drives in all computers to be surplus outside the government, except for those to be reallocated to the Computers for Schools program.

Care should also be taken in the return or disposal of devices, such as facsimile machines, scanners and photocopiers, that retain information in memory.

For public bodies subject to the Records Management Regulation, destruction of information must take place in accordance with the records management policies and procedures established by the Government of Alberta. Surplus Sales, Service Alberta offers services to these public bodies for the wiping clean of computer hard disks before their disposal.

See *Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices* and *Security Policy for Disk Wiping Surplus Computers*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

Disposing of transitory records

A policy, records schedule, bylaw or other instrument should set rules for retention and disposition of records, including transitory records, so individual employees can decide which records should be retain and which records can be destroyed.

A *transitory record* is a record that has only immediate or short-term usefulness or value and will not be needed again in the future. Transitory records contain information that is not required to meet legal or financial obligations or to sustain administrative or operational functions, and has no archival value.

Transitory records are defined for provincial public bodies in the Transitory Records Schedule, approved under the Records Management Regulation. Guidelines for retention and disposition of transitory records can be found in *Official and Transitory Records: A Guide for Government of Alberta Employees*, published by Records and Information Management, Service Alberta.

Local public bodies may develop and approve their own definitions, but must be prepared to explain to the Commissioner why they believe that certain records are transitory records.

Some examples of recorded information that may be managed as transitory records are

- information of short-term value (e.g. personal messages, notes kept to prepare official minutes of a meeting);
- duplicate documents (where nothing has been added, changed or deleted; the copies have been used for reference or information purposes only; and the master version of the document has been filed in an official filing system);
- draft documents and working materials that are used to create a master record, except for drafts of legislation, legal documents, budgets, policy changes or changes in decisions;
- advertising material (including spam);
- external publications;
- e-mail containing personal messages and routine announcements, but not recommendations, decisions or transactions by public bodies. Public bodies should have an internal e-mail policy that aids officials and employees in deciding when e-mail messages should be retained in records systems; and
- voice-mail messages, unless it is necessary to document a decision or transaction recorded on voice-mail.

Organizing, storing and protecting recorded information

A policy that establishes a records system will provide a framework for the organization and storage of recorded information that facilitates the location and retrieval of the information. The policy should also address information security and the protection of personal information, both for business and FOIP purposes.

The public body should have guidelines and procedures in place relating to the organization, control, storage, and protection of recorded information, including electronic records. *IPC Order 2000-020* states that a public body must have an adequate records management system in place to keep track of all internal uses and external disclosures of records and information as part of its duty to protect personal information.

For government public bodies, see also *Government of Alberta Information Technology Security Policy* and *Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta, as well as *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta.

Organizing and storing electronic records

Electronic records include both data-based records (i.e. numbers and text in structured fields of databases) and document-based records (i.e. correspondence created in word processing or other applications, web pages, graphical objects and e-mail). Electronic records are subject to the *FOIP Act* and should be managed throughout their life cycle as part of any program for the management of recorded information.

Ideally, in an electronic records system, processes should be in place to ensure that

- individual records are uniquely identified;
- contextual data, or “metadata,” relating to the specific record or transaction is preserved (this may consist of, for example, date, subject, names of correspondents or participants);
- records can be authenticated;
- there is version control;
- records are classified and indexed for retrieval;
- there are access controls;
- there are controls over the alteration of records;
- there is the ability to audit access to and alteration of records; and
- there are processes in place to permit the disposition of records, including e-mail, under approved records schedules using secure processes.

If the public body does not have an adequate electronic records system, its records management policy should require records to be printed and managed as part of the records system used to manage hard-copy records.

Provincial government departments and **Schedule 1** public bodies may refer to *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta, for further information and assistance.

Including routine disclosure practices and privacy requirements in the planning and design of electronic information systems

There are two special needs of public bodies that require special information management standards and specifications. These should be considered in the design of electronic information systems.

First, routine disclosure of recorded information outside the *FOIP Act* should be supported. Recorded information should be managed to promote public access where this is appropriate. It may be desirable that electronic information systems include a

public access component. Public bodies should ensure that opportunities for routine access are considered in the design and functional specifications for new or modified electronic information systems. This will facilitate routine disclosure and active dissemination of information, where appropriate, after the system is implemented.

Second, privacy protection measures must be considered in the design and functional specifications for information systems that are used to collect, generate, manipulate, and disclose personal information. The particular requirements for protection of privacy in this area are discussed in Chapter 9.

Managing recorded information in contracting

When public body programs or services are provided by contractors or other agencies, a policy for managing recorded information should state that all contracts require the contractor to create records that meet the public body's requirements.

Contracts should also require the contractor to maintain records according to standards acceptable to the public body for as long as required, to dispose of the records according to standards acceptable to the public body, or to return records to the public body, as appropriate.

When activities requiring the collection or handling of personal information are contracted out, the contract should set out the privacy protection and security obligations assumed by the contractor (see Chapter 9).

Conditions governing FOIP and records management as they relate to contracting are further explained in the publication *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

8.5 Records Issues Relating to Access Requests

The right of access to records provided in the *FOIP Act* is intended to make public bodies more open and accountable to the public. Inadequate record-keeping can contribute to poor accountability to clients and the general public.

In the case of FOIP requests, a public body may find that poor records and information management can cause it to contravene the Act. This may lead to damage to the public body's credibility and reputation. Some common issues that arise in the context of access requests are the ability to locate records, adequate standards of documentation, disposition of records, and disclosure outside the Act.

Ability to find records

The access provisions of the *FOIP Act* assume that public bodies can identify, locate and produce records in response to requests. This ability is crucial both in making information routinely available to the public and in responding to FOIP requests.

The search process is greatly facilitated if a retrieval system is in place that allows staff processing an access request to search for a particular topic or subject and find all locations where records may be kept and also find the records in any media.

The failure to capture records in effective records systems is the most commonly cited problem associated with inadequate management of records and information. (See, for example, *IPC Order 97-019* and *IPC Investigation Report 98-IR-009*.)

This failure may result in difficult and time-consuming searches for records, as well as uncertainty that all records relevant to a FOIP request have been located. This is particularly an issue when no records can be found on a subject, although it appears that a public body should have created and maintained records on the subject and there is no evidence that the records were disposed of in an authorized manner.

Applicants frequently challenge the adequacy of a search for records by a public body. Public bodies will find it easier to demonstrate thoroughness if there is an established records system. For an example of the analysis of a public body's records system and its search for apparently missing records, see *IPC Order 98-003*.

Public bodies also need to be able to show that a search for records has been conducted in a systematic and reasonable manner. The Information and Privacy Commissioner has stated that a search that relies solely on the memory of an employee is not in compliance with the Act (see *IPC Order 99-021*). The Commissioner has also ruled that a limited "keyword" search does not constitute an adequate search (see *IPC Order 99-002*), and that public bodies should be able to locate all records that are "reasonably related" to the applicant's request (*IPC Orders 97-020* and *99-002*).

On the other hand, a public body is not required to inform an applicant of the existence of records in other public bodies, to provide indexes to files that have not been requested, or to provide an applicant with records retention and disposition schedules (unless this is part of the access request) (see *IPC Order 99-039*).

An effective records system should allow retrieval of semi-active as well as active records (see *IPC Order 96-021*). It should also allow retrieval of inactive records in a storage facility, such as the Alberta Records Centre (for provincial government departments and **Schedule 1** public bodies). The Commissioner has found that there may be a requirement to search and access electronic back-up tapes, depending on the circumstances of a case (*IPC Order F2007-028*).

In addition, the records system should provide some ability to alert an applicant to the fact that records may have been transferred to the public body's archives (see *IPC Order 96-022*).

In *IPC Order 2000-020*, the Commissioner stated that adequate records management under the Act involves keeping track of all internal uses and external disclosures of records and information relating to clients' medical information. In that Order, the Commissioner suggested that the public body should have kept a precise list of the medical records that were provided or summarized for a consultant's review in evaluating a compensation claim.

Adequate documentation

Employees of public bodies are accountable for documenting their activities or transactions. Although the *FOIP Act* does not impose requirements as to how a public body should structure or maintain its records system (see *IPC Order 2000-030*), a public body should have clear direction from senior management as to how officials and employees will document business activities of the public body.

As well, there is a need in the modern electronic work environment to ensure version control, so that public bodies can retrieve the authoritative versions of documents. If information technology systems do not have version control capability, practices should be developed to identify authoritative versions of documents.

This kind of direction may help to reduce situations where records are not created to a standard adequate for the public body's needs or where it is impossible to determine the authoritative version of a record on which a decision or other action was based.

There is also need for clear direction on what records the public body considers to be transitory. In the absence of such direction on transitory records, the Commissioner may require a public body to produce other evidence at an inquiry that a record that has been destroyed was appropriately destroyed as a transitory record (see *IPC Order 99-009*). Transitory records are discussed in greater detail in section 8.4 of this chapter.

Finally, guidelines for employees should clearly indicate that the official records of the organization cannot be altered or destroyed without authorization. Alteration or destruction of records is a very serious matter, especially when done to evade a FOIP request, and could lead to penalties or sanctions. See Chapter 2, section 2.11 for information on the offence provisions of the Act.

Controls over disposition

Cost-effective business practices include having a systematic process for evaluating and disposing of records as they become inactive and are no longer needed for business purposes, for the operations of the public body (e.g. to protect the public body's interests in the event of litigation) or for long-term preservation.

Establishment of records retention and disposition schedules, and compliance with them, allows public bodies to set accurate limits to searches for records.

This process, known as records scheduling and disposition, has several advantages from a FOIP perspective. First, properly authorized retention and disposition schedules provide an official approval process for the destruction of records, including transitory records, based on business needs. Schedules also provide evidence for the applicant, and for the Commissioner if necessary, that records have been appropriately disposed of by the public body.

The Commissioner has emphasized the importance of rules relating to the destruction of records, and he has noted that it is within the purview of the Commissioner to ensure compliance with such rules (see *IPC Order 98-011*).

Second, schedules identify what records of enduring value should be transferred to the Provincial Archives of Alberta or other archives. See section 7.7 of Chapter 7 for

a discussion on disclosure of personal information to archives, including the transfer of information to an archival facility that is not a public body, but which has a contract or agency relationship with a public body (**section 40(1)(p)**). FOIP requests can then be dealt with on behalf of the public body by these organizations, which are usually well-placed to deal with requests for records.

Third, schedules allow for the movement of records as their value changes. This reduces the need for public bodies to tie up resources in the maintenance of older records, which may be very labour-intensive to locate and handle. Older records that are needed to record the activities of a public body, to protect its interests or to provide long-term corporate memory for the public body can be placed in the Provincial Archives of Alberta, the archives of a public body, or other archival facility, as appropriate.

Fourth, schedules provide controls over the disposal or destruction of records, so that public bodies know what was destroyed, and when. Adequate documentation related to the destruction of records may also provide useful documentary evidence in the event of a Commissioner's review. In *IPC Order 99-021*, the Commissioner noted that, if records have been destroyed in accordance with approved records retention and disposition schedules, the public body must inform the applicant of the relevant destruction certificate numbers in its response.

Ability to routinely disclose records outside the FOIP process

A public body needs to have effective control over the records and information it collects and creates and to be knowledgeable about such records and information. This is required to make effective decisions about which records should either be released on a routine basis or actively disseminated to the public.

Routine disclosure and active dissemination are practices that contribute significantly to openness in public administration, better client service and more effective mechanisms to reduce the number of FOIP requests under **Part 1** of the Act. For further information on routine disclosure of records and information, see section 2.4 of Chapter 2.

