



DRUMHELLER

COUNCIL POLICY



COUNCIL POLICY # C-7-99

RECORDS MANAGEMENT POLICY

POLICY STATEMENT:

In order to bring information systems into compliance with the privacy provisions of the Freedom of Information and Protection of Privacy Act, the Town of Drumheller will:

- 1) Support and provide for the public's right to know what personal information is collected and how it will be used and the right of individuals to access their own personal information;
- 2) Protect personal information in its custody or under its control protected from unauthorized collection, use, or disclosure;
- 3) Ensure that the Town's electronic and hard copy records filing systems will comply with F.O.I.P. legislation.
- 4) Contribute to the highest quality of management and effectiveness for both the electronic and hard copy records filing systems.

Control Over Records Storage

Each department shall be responsible for the maintenance of their own filing areas. Records will be managed so that they are easy to store and retrieve, and secure against loss or unauthorized access, both electronically and in the hard copy filing system. Each department shall appoint a records administrator to ensure consistent implementation of FOIP and the records management policies and procedures.

Each department shall maintain their records as follows:

- 1) On an annual basis, the files from the previous year(s) shall be reviewed for retention purposes (Refer to Schedule for Retention and Disposition of Inactive Records Policy No. C-4-99 and Transitory Records Disposal Policy No. C-5-99);
- 2) The retention period pertaining to each record for that year shall be recorded on the file list. Each department shall develop a method of identifying permanent records. Permanent records are those that will eventually be transferred to the vault

for archive purposes.

- 3) Departments shall review records and perform archiving annually if required. All records transferred to archives must be listed with the F.O.I.P. Coordinator;
- 4) The department head must sign off the list of all files that are to be destroyed with a copy forwarded to the F.O.I.P. Coordinator.
- 5) Each departmental file list of records will be given to the F.O.I.P. Coordinator to update the records database annually.
- 6) On an annual basis, the electronic files shall be reviewed and all inactive documents shall be deleted from the system in conjunction with the Systems Administrator.
- 7) All sensitive records (confidential in nature) stored electronically shall be secured against unauthorized access with the use of passwords.
- 8) All hard copy sensitive records shall be marked as such and secured against unauthorized access.

Control Over Copies

The original of any record (refer to F.O.I.P.'s definition of record) shall be filed with the end user. In order to control duplication of file copies, the following stamp must be applied to the original document prior to any reproduction of copies:

Copies made: _____
To: _____
Original will be filed: _____

Rule: an original should always be forwarded to the end user for retention.

Records Database

A records database shall be maintained under the direction of the F.O.I.P. Coordinator.

Electronic Records Backup Tapes

The daily electronic backup tapes shall be stored in a secured location. One backup tape must be stored off site in a secured location. The off-site backup tape must be exchanged at least once per week.

Information Protection

The F.O.I.P. Act defines **Personal Information** as recorded information (whether electronic or hard copy) about an identifiable individual which includes but is not

limited to name, address, telephone number, race national or ethnic origin, color, or religious or political beliefs or associations; age, sex marital or family status, identifying number, health, physical and mental information, educational, financial employment, or criminal history, anyone else's opinion about the individual and the individual's personal views or opinions, except if they are about someone else.

Section 36 of the F.O.I.P. Act - The local body must protect the personal information contained in the Personal Information Bank (PIB) by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

- 1) Personal information **must not** be given to third parties which includes utility companies, banking institutions, barristers and solicitors, etc. without the consent of the individual or pursuant to the allowable disclosures provided for in Section 38 of the F.O.I.P. Act.
- 2) Personal information of an individual **must not** be visible to the public.
- 3) Personal information **must not** be made available to the public, co-workers or elected officials. Only authorized employees (those individuals which require the personal information in order to perform their assigned duties) shall access personal information. RULE: "Need to know" principle. All requests for personal information must be directed to the head of the local body, Chief Administrative Officer.
- 4) The public **must not** have access to computers unless it is a computer that has been designated for public access use.
- 5) Personal information **must not** be left on the computer screen while an employee is away from his working station.
- 6) Personal information may be exchanged on the fax machine or through E-Mail externally only if secure arrangements are in place with the recipient.
- 7) The minimum amount of personal information required to carry out a program or activity shall be collected. "Need to know" principle.
- 8) Personal information shall be collected directly from the individual unless indirect collection is authorized as stated in the F.O.I.P. Act (Section 33(1)(a) to (k)).
- 9) Personal information shall be secured, i.e. locked rooms, storage cabinets, and controlled access to computers.

Accuracy of Personal Information

Section 34(a) and 35 of the F.O.I.P. Act - A public body must make every reasonable effort to ensure that personal information used to make decisions that affect an individual is accurate and complete.

- 1) Personal Information shall be reviewed for any errors or omissions by the individual as requested. All requests to review personal information must be by the

individual whom it is about and directed to the head of the public body, Chief Administrative Officer.

2) Corrections or annotations in the case of error or omissions must be made by written request to the Chief Administrative Officer.

3) Where necessary, a notification of a correction or annotation of personal information will be sent to any other public body or third party to which the information has been disclosed during a one-year period prior to the correction or annotation.

4) Personal information collected shall be verified for accuracy with the electronic system.

Disclosure Statements for the Collection of Personal Information

A disclosure statement **must be** printed on all information forms where personal information is being collected. The reason for the request of personal information must be disclosed to the person as to how the information he or she is providing will be used. The statement will reference a "business function" as listed below:

- Parks, Recreation and Cultural
- Assessment and Taxation; Utilities; Public Works; Solid Waste Services
- Bylaw Enforcement, Licensing and Inspections
- Development Control, Land Use Planning and Safety Codes Permits
- Internal Services (Finance and Human Resources)

For example: The following statement will be printed on all Community Services Department forms:

*"Personal Information is being collected for the purpose of **Parks, Recreational and Cultural**" pursuant to the provisions of the Municipal Government Act and its regulations, and pursuant to Section 32(c) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of your personal information, you may contact the appropriate DEPARTMENT HEAD or the F.O.I.P. Coordinator at (403)823-1339.*

Effective October 1, 1999, all forms that request personal information must include a F.O.I.P. statement. Forms that do not require reprinting prior to this date will require an attachment containing the F.O.I.P. statement (via stamp, brochure or printed attachment).

Wherever possible, personal information shall be collected from the individual in person, however there will be occasions when the personal information may be obtained by telephone. In these occurrences, the disclosure statement will be given to the individual by verbally over the telephone.

All employees shall only use or disclose the personal information collected for the purpose it has been collected unless otherwise allowed pursuant to Section 38 of the F.O.I.P. Act.

Retention of Personal Information

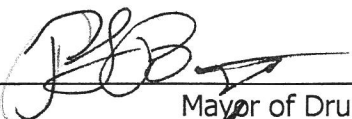
Section 34 (b) of the F.O.I.P. Act - If information has been used to make a decision that directly affects an individual, the information must be retained for at least one year after use. Example: Job applications; Revenue Canada inquiries; etc.

Personal Information Bank and Public Information Directory

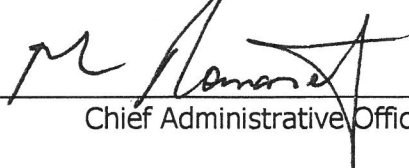
Both lists shall be given to the public upon their request.

Adopted by Council

Date: September 13, 1999



Mayor of Drumheller



Chief Administrative Officer