

Privacy Protection Policy

SECTION	Administration	POLICY NUMBER	2-3-13
SUB-SECTION	Information Management	EFFECTIVE DATE	November 15, 2016
SUBJECT	Privacy Protection		
AUTHORITY	Senior Management - November 15, 2016		

1. Purpose

In order to provide public accountability and transparency of its services, and to protect Dufferin County staff and the public, this policy outlines the standards and procedures for the collection, use, disclosure, retention and disposal of recorded personal information. This Policy also sets out the conditions in which personal information may be disclosed along with the proper procedure to follow in the event of a privacy breach.

This policy is in support of the Strategic Plan Priorities and Objectives::

- 3.2 Increase transparency
- 3.3 Improve policies, practices and procedures

2. Dufferin Statement

In accordance with its obligations under the *Municipal Freedom of Information and Protection of Privacy Act* (“MFIPPA”) and *Personal Health Information Protection Act* (“PHIPPA”) (together, the “Acts”), the Corporation of the County of Dufferin (“Dufferin County”) will ensure the protection of individuals’ personal information in its custody or control by complying with the appropriate methods for the collection, use, retention and disposition of personal information, online or offline, as much as is reasonably possible.

3. Definitions

Dufferin County adheres to the following definitions from the Municipal Freedom of Information and Protection of Privacy Act and Personal Health Information Protection Act:

Personal Information: means recorded information about an identifiable individual, including,

- a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- b) Information relating to the education or the medical, psychiatric; psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- c) Any identifying number, symbol or other particular assigned to the individual;
- d) The address, telephone number, fingerprints or blood type of the individual;
- e) The personal opinions or views of the individual except if they relate to another individual;
- f) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- g) The views or opinions of another individual about the individual; and
- h) The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

(Municipal Freedom of Information and Protection of Privacy Act, s. 2)

Personal Information Bank (PIB): means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual

(Municipal Freedom of Information and Protection of Privacy Act, s. 2)

Personal Health Information: means identifying information about an individual in oral or recorded form, if the information:

- i) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family
- j) Relates to the providing of health care to the individual, including the identification of a persona as a provider of health care to the individual,
- k) Is a plan of service within the meaning of the Home Care (Personal Health Information Act)

(Personal Health Information Protection Act, s. 4)

Privacy Audit: is an assessment or examination of current policies, procedures, and practices related to the collection, use, retention, and disclosure of personal information in any format or medium.

Privacy Breach: occurs when personal information is collected, retained, used, or disclosed in a way that is not in accordance with MFIPPA.

Privacy Impact: is anything that could jeopardize or negatively impact an individual's privacy. A privacy impact can, for example, take other forms such as fraud, physical safety issues, such as stalking or harassment, financial loss, adverse impact on employment or business opportunities, or damage to reputation.

(Information and Privacy Commissioner's Office, Privacy Impact Assessment Guidelines, pg 16)

Privacy Impact Assessment (PIA): is a process for identifying, assessing and mitigating privacy risks.

(Privacy Act, Appendix A)

Records: any recorded information, whether in printed form, on film, by electronic means or otherwise, including: correspondence, memoranda, plans, maps, drawings, graphic works, photographs, film, microfilm, microfiche, sound records, videotapes, e-mail, text message, machine readable records, and any other documentary material regardless of physical form or characteristics, and including "official records" and "transitory records".

(Personal Health Information Protection Act, s. 2)

4. Scope of Responsibility

4.1 General Conditions

The following conditions apply to the collection of personal information, in relation to the individual providing it:

- Dufferin County may only collect personal information that relates directly to its operating programs or activities;
- Wherever possible, personal information should be collected directly from the person it concerns, and Dufferin County shall make all reasonable attempts to inform the individual about the purposes of collection;
- Dufferin County will work with the individual to ensure that all information collected is accurate, up-to-date and complete;
- Dufferin County shall only use personal information for the purposes for that which it was collected, or for a purpose consistent with the original request;
- Dufferin County will not share, sell, rent, distribute or otherwise disclose or disseminate personal information to any organization or individual outside of Dufferin County and,
- Personal information may be disclosed without an individual's consent, permitted by the Acts, in the following cases:
 - In the event that a third party must be contracted to process the request;

- For mandatory law enforcement purposes (such as warrants, court orders and proceedings of the like);
- Where the disclosure is authorized by federal legislation and,
- Where public interest in disclosure outweighs the invasion of privacy.

Dufferin County does not use or retain personal information provided for any secondary purposes unless the individual in question has been notified and has provided permission to do so.

4.2 Individuals

Under MFIPPA, an individual has the right to see the information that Dufferin County holds about them, and to request corrections to that information.

To do so, a Freedom of Information (FOI) Request must be made in the relevant government department or agency.

Dufferin County's FOI form can be found here:

<http://www.dufferincounty.ca/files/content-pdf/dufferin-foi-request.pdf>

4.3 Employees

Dufferin County staff (employees, volunteers, agents, or contractors) shall take all reasonable measures to protect against theft, loss, unauthorized use, and mistaken disclosure of any personal information.

Every employee shall ensure that any record containing personal information are disposed of in a safe and secure manner and in accordance with the Acts.

Employees who do not comply with this policy may be subject to progressive discipline up to and including termination of employment.

5. Collection of Personal Information

Dufferin County adheres to the following procedures regarding personal information collection:

- 5.1** Personal information will not be collected by Dufferin County staff unless essential for business purposes or authorized for collection under legislation, or Dufferin County bylaw

- 5.2** A Privacy Impact Assessment (PIA) will be conducted for:
- a) Any new administrative program or new type of municipal service collecting, storing or using personal information;
 - b) Significant changes made to an existing program or service such as conversion from a paper to electronic system or changes to the type or amount of personal information collected etc;
 - c) Significant changes to technology based business applications or implementation of new systems, which collect or retain personal information;
 - The privacy impact assessment will be completed by staff implementing the program or service and reviewed by the supervising Manager or Director
 - The completed PIA will be provided to the Information Management Coordinator for review
 - See Appendix B i. for the Privacy Impact Assessment form and Appendix B iii. for the guidelines for completing the assessment
- 5.3** When personal information is collected there will be a 'notice of collection' statement setting out: the legal authority for collection, the principle purpose of collection, the title, business address, and contact information of the responsible employee or department. See Appendix C for the Notice of Collection Template.
- 5.4** This statement will be provided on all written or electronic forms collecting personal information, will be available upon request when personal information is collected verbally, and will be clearly posted in municipal facilities where necessary;
- 5.5** Personal information will not be collected without the knowledge or consent of the individual to whom the information relates except in certain conditions under s.29 of MFIPPA or when providing emergency care or treatment
- 5.6** Personal information of minors (under 16) will not be collected without express or implied authorization of a parent/guardian except in the cases of providing emergency treatment; and
- 5.7** All personal information collected will be complete and accurate.

6. Web Privacy

The interaction between individuals and the Dufferin County website are strictly non-identifiable and comply with previous claims that no personal information shall be gathered without prior consent. Dufferin County's website does gather and store data but does not identify individuals personally. This data is used for analytics to garner a better understanding of matters of importance to residents and the public and to ultimately make the website more user-friendly.

The site does use session-based, or temporary, cookies that are created with a user visits the site, but they are automatically deleted.

The County of Dufferin uses SSL encryption technology to protect personal information on applications that require personal information. This includes identifiable information as well as credit card numbers. A security icon will appear on the browser of the user to indicate entering onto a secure site.

Dufferin County is not responsible for the privacy practices of websites beyond our own. This privacy policy applies solely to the information collected while on the County's website.

7. Privacy Audits

A privacy audit will be conducted on an as needed basis to evaluate employee knowledge and execution of Dufferin County's privacy related policies and procedures by the Information Management Coordinator.

8. Privacy Breach General Procedure

In the event of a privacy breach, Dufferin County will take the following steps:

8.1 Step 1: Identify

If a complaint has been received or there is a suspicion that there is a privacy breach, contact the Information Management Coordinator or their designate immediately. The concern can be from a member of the public or from internal staff. The Information Management Coordinator will evaluate and determine if a privacy breach has occurred. If a privacy breach is confirmed, the Information Management Coordinator will proceed accordingly.

8.2 Step 2: Contain

The first priority after a confirmed privacy breach is to contain the damage as much as is reasonably expected. The Information Management Coordinator will work with the necessary departments to identify the scope of the breach and will take steps to contain it by:

- Retrieving any hard or electronic copies of personal information that has been disclosed;
- Ensure there are no unauthorized duplicates of personal information;
- Prevent unauthorized access to more files by taking the necessary steps (such as changing keys, resetting passwords, suspend access, system shut down, etc.)

8.3 Step 3: Notify

The Information Management Coordinator will proceed to notify all individuals involved or affected by the breach via telephone call or by a formal letter. The content will include the following information:

- Any relevant information surrounding the nature of the alleged, or confirmed, breach;
- Details of the breach that is available at the time of the notification;
- Specific areas that were affected;
- Procedures that are underway to contain, control and reduce harm of the breach;
- Steps an individual should take to protect themselves;
- Future steps to prevent a similar incident; and
- Contact information about the Information Privacy Commissioner's Office in case of further questions.

8.4 Step 4: Investigate

Once the breach has been contained and all individuals notified, the Information Management Coordinator will work with the necessary departments and their staff to undertake an investigation to establish:

- The extent of damage of the privacy breach (sensitivity, number of individuals affected etc.);
- The source of the breach, including future preventative measures, if able;
- A time line of events that has led to the breach; and
- Any other relevant information relating to the circumstances, before or after.

The Information Management Coordinator will report the breach to the Information Privacy Commissioner and, depending on the breadth of damage, may work in consultation with the Information Privacy Commissioner office to investigate.

8.5 Step 5: Report and Follow-Up

Following the completion of the investigation, the Information Management Coordinator will release a report outlining the results of the investigation. This report will also include recommended steps to prevent another breach for the future as well as steps on how to mitigate damage. The report will be forwarded to the Information Privacy Commissioner as well as all individuals who were affected. The report shall be included on the agenda of the General Government Services Committee if:

- More than five (5), individuals are affected by a confirmed breach; or
- In the opinion of the Municipal Clerk that it would serve the public interest to provide such a report

Any recommendations within the report will be reviewed and implemented, if appropriate.

**Appendix A - Procedures for the Collection, Retention
and Disclosure of Personal Information to
County of Dufferin
Privacy Protection Policy**

Retention of Personal information

1. Personal Information will be retained for one year after it is collected or used unless authorized under another retention period in the Classification and Retention Schedule bylaw 2014-06
2. All personal information whether in paper or electronic form will be retained in a safe and secure manner.

Use and Disclosure of Personal Information

1. All personal information banks maintained by the County will be kept as accurate and up to date as is reasonably possible. All personal information banks will be identified and the resulting listing shall be made available to all employees and the public upon request.
2. Personal information will only be used for the purpose for which it was collected unless for a 'consistent purpose' the individual to whom the information relates might reasonably expect, or unless authorized under statute or policy;
3. The use and disclosure of personal information for any purpose other than the one for which it was collected will only be permitted with the consent of the individual to whom the information relates, or in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act;
4. Access to personal information will be restricted to only those employees requiring access in order to carry out their duties;
5. Personal information will not be left exposed or visible on desks or computer screens;
6. Records containing personal information shall not be removed from the workplace unless authorized under another policy or statute. External and mobile devices containing or accessing personal information will be kept secure and managed according to Dufferin County's Mobile Device Acceptable Use Policy; and
7. Sensitive, personal or confidential information should wherever possible, be sent by regular mail or courier. If transmitting such information by email or fax, addresses and fax numbers must be verified to ensure that they are accurate.

**Appendix B - Procedures for Staff Access to Human Resources Personal
Information
County of Dufferin
Privacy Protection Policy**

All personal information maintained by Human Resources is collected, used and maintained in accordance with Appendix B and as outlined in the Consent to the Collection, Use and Disclosure of Personal Information Form. The following procedures outline how staff can access their personal information as maintained by the Human Resources Department.

1. Employees can request access to their own information by calling their Human Resources representative and making arrangements to access their personnel and medical files in Human Resources. The meeting must be scheduled in advance at a mutually agreeable time. (Human Resources may ask the employee to show identification if necessary.)
2. Employees shall be granted access to information contained within their personnel files except under certain limited circumstances.
 - a. A supervisor's notes may contain witness statements or other information for use in investigations.
 - b. In the case of a recruitment process, employees may request feedback from their HR representative.
3. Employees will not be provided access to:
 - a. Records dealing with Labour relations matters;
 - b. Records related to investigations.

**Appendix C – Notice of Collection Template to
County of Dufferin
Privacy Protection Policy**

Please find below a template for wording that should be completed and placed on any form - paper or electronic that collects personal information. This must be available to the public either electronically or in hard copy. Please note that anything in yellow needs to be made applicable to each form. This is the minimum amount of information required. If there is additional information that can be provided this template can be modified. The template can be merged with a statement of waiver or confidentiality.

Collection Notice: The personal information collected on this form is collected under authority of (Municipal Act or Applicable Legislation or By-law). This information will be used to (Insert purpose for collection and all possible uses). Questions about the collection of personal information should be directed to the [redacted] or reached at 519-941-[redacted]xxxx (phone extension).