Newmarket

CORPORATE POLICY

Sub Topic: Protection of Personal Information	Policy No. CORP. 1-08
Topic: Corporate Records	Applies to: All Employees
Section: Legislative Services	Council Adoption Date: May 5, 2014
Effective Date: May 5, 2014	Revision No: Date:

Policy Statement & Strategic Plan Linkages

The collection and use of personal information about Newmarket residents and other members of the public is a necessary part of the Town's regular business processes. Part II of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) requires institutions to use appropriate methods for the collection, use, retention and disposition of personal information.

This Policy relates to the key area of focus: "Well-Equipped and Managed" of the Strategic Plan. The collection, use and management of personal information in a responsible and transparent manner links directly to the Core Values of Accountability and Accessibility.

Purpose

In order to provide greater accountability and to protect the privacy of staff and the public, this policy outlines the standards and procedures for the collection, use and management of personal information by all Town employees. This policy applies to all personal information, personal health information and personal information banks which are collected and maintained by the Town of Newmarket.

Definitions

Personal information
Personal Information Bank (PIB)
Personal Health Information
Privacy Audit
Privacy Breach
Privacy Impact Assessment (PIA)
Records

Procedures

1. Personal information will be collected, used and retained in accordance with MFIPPA and other privacy legislation and all related procedures attached as Appendix B.
2. A privacy audit will be conducted for the Corporation every two to three years by the Legislative Services Department to evaluate employee knowledge and execution of the Town's privacy related policies and procedures. Interim audits will be conducted on an as needed basis for individual departments or business units. The Audit will be conducted according to the procedures attached as Appendix C.
3. All privacy complaints and either suspected or evident privacy breaches will be reported immediately according to the procedures in Appendix D.
4. All personal information about Town employees will be collected used and retained in accordance with Appendix B and Appendix F.

Responsibilities of Employees

All Town of Newmarket employees shall take all reasonable measures to protect against theft, loss, unauthorized use, and unauthorized disclosure of any personal information.

All employees shall ensure that all records containing personal information are disposed of in a safe and secure manner and in accordance with the Records Retention Policy CORP.1-06.

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

Responsibilities of Management

All supervisors, managers, directors, and commissioners must maintain all personal information of staff and the public in accordance with the established procedures in this policy.

Cross-References

Alternative Work Arrangement Policy HR.2-07
Employee Code of Conduct Policy CAO.3-01
Municipal Freedom of Information and Protection of Privacy Act, R.S.O., 1990, C. M.56
Personal Information Protection and Electronic Documents Act S.C. 2000, c.5
Records Retention Policy CORP.1-06
Routine Disclosure and Active Dissemination Policy (TBD)
Risk Management Policy (TBD)
Video Surveillance System Policy (TBD)
Use of External and Mobile Devices Policy (TBD)
Harassment and Discrimination Free Workplace Program
Violence Free Workplace Program

Appendices (which may be amended from time to time)

Appendix A - Definitions
Appendix B - Procedures for the Collection, Retention and Disclosure of Personal Information
- Appendix B.i - Privacy Impact Assessment Form
- Appendix B.ii - Privacy Impact Assessment Guidelines
- Appendix B.iii - Notice of Collection Template
- Appendix B.iv - Personal Information Bank Listing - Town of Newmarket (TBD)

Appendix C - Privacy Audit Procedures
Appendix D - Privacy Breach/Complaint Procedures
Appendix E - Website Privacy Policy
Appendix F – Procedures for Staff Access to Human Resources Personal Information

Appendix A – Definitions
To
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

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)

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)

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

a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
b) 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,
c) is a plan of service within the meaning of the Home Care

(Personal Health Information Protection Act, 2004 S.O. 2004 C.3 Sched. A, section 4)

Appendix A – Definitions
To
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

Privacy Audit means 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 Assessment (PIA) is a process that helps determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements;

Records means 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”;

Appendix B - Procedures for the Collection, Retention and Disclosure of Personal Information
to
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

Collection of Personal Information

1. Personal information will not be collected by Town staff unless essential for business purposes or authorized for collection under legislation, or Town bylaw;
2. A Privacy Impact Assessment (PIA) will be conducted for:
   - any new administrative program or new type of municipal service collecting, storing or using personal information;
   - 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; and
   - significant changes to technology based business applications or implementation of new systems, which collect or retain personal information;
     a. The privacy impact assessment will be completed by staff implementing the program or service and reviewed by the supervising Manager or Director;
     b. The completed PIA will be provided to the Records and Projects Coordinator;
     c. See Appendix B.i for the Privacy Impact Assessment form and Appendix B.ii for the guidelines for completing the assessment;
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 B.iii for the Notice of Collection Template.
   a. 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;
4. Personal information will not be collected without the knowledge or consent of the individual to whom the information relates except in certain exceptions under s. 29 of the *Municipal Freedom of Information and Protection of Privacy Act* or when providing emergency care or treatment;
5. Personal information of minors (under 16) will not be collected without express or implied authorization of a parent / guardian except in the case of providing emergency treatment; and
6. All personal information collected will be complete and accurate.

Appendix B - Procedures for the Collection, Retention and Disclosure of Personal Information
to
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

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 (Appendix F of the Records Retention Policy CORP. 1-06); and
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 Town 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. See Appendix B.iv;
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 s. 31 and s. 32 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 data security and governance 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.

Privacy Impact Assessment

Appendix B.i of Protection of Personal Information Policy CORP.1-08

Date

Name of Program or Service

Name of Author

Newmarket

Privacy Impact Assessment

1. Introduction

a) Name of Program or Service

b) Name of Department, Branch and Program Area

c) Name of Program or Service Representative

d) Key Program or Service Dates

2. Description

a) Summary of the New Program or Service or Change

b) The Intended Scope

c) Conceptual Technical Architecture (if applicable)

d) Description of Information Flow (include text and diagram to describe flow as necessary)

3. Collection, Use and Disclosure of Personal Information

NOTE: Tables would be helpful to organize the answers to (a), (b), (c), and (d)

a) Authority for the Collection, Use and Disclosure of Personal Information

b) **List of Personal Information to be Collected, Used and/or Disclosed, the Method of Collection and Disclosure, and the Rationale for each**

c) **The Sources and Accuracy of the Personal Information**

d) **The Location of the Personal Information**

e) **The Retention Schedule and Method of Destruction or De-identification for Personal Information**

f) **Identification of Consent Issues**

g) **Users of Personal Information**

4. Access Rights for Individuals to their Personal Information

5. Privacy Standards: Concerns and Security Measures

a) **Security Safeguards**

b) **Avoidance of Unintentional Disclosure**

6. Conclusions

a) An Assessment of the Impact on Privacy, Confidentiality and Security of Personal Information as a Result of the New Program or Service or Change

b) Strategy for Mitigation of Privacy Risks

c) Additional Comments

Approved By:

Employee (Author)

Manager / Director (or designate)

Town Clerk (or designate)

Form to be submitted to Legislative Services for approval.

Appendix B.iii – Notice of Collection Template
to
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

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 (Insert Position Title), or reached at 905-953-5300 ext. (phone extension).

The contact information should refer to a manager or a supervisory position within the applicable department that can respond to specific questions regarding the use of the information. Questions specific to the Municipal Freedom of Information and Protection of Privacy Act, or relating to the disclosure of information can be directed to the Records and Projects Coordinator.

Guide for Completing a Privacy Impact Assessment

Appendix B.ii of Protection of Personal Information Policy CORP.1-08

Notes:

- This Guide is intended to assist you with the completion of the Privacy Impact Assessment.
- When completing the Assessment, keep in mind that not all questions will be relevant to your project at this time.
- If a question is not applicable, answer “Not applicable,” but do not delete the question from the Assessment.
- Add additional questions and/or explanations as required by your project.
- Attach any relevant documents.
- Where appropriate, provide information on both the current plan, and future intentions for the program/service.
- “Change” means a change to a program or service that affects the collection, use, disclosure or retention of personal information and includes the implementation of an information system.
- It is important to remember your audience for this assessment. It is not intended to be an assessment of the technical architecture of the system, but an assessment of privacy issues arising from a change. Make an effort to keep information straightforward and understandable by a reader who does not have expertise in information system technology, law, or the background to the system.
- Avoid jargon and acronyms unless they are explained.
- Explain any terms, positions and organizations that are not commonly understood.
- Although information must be comprehensive, make an effort not to include information that is not necessary to the reader’s understanding of the change and its impacts.

1. Introduction

a) Name of Program or Service

b) Name of Department, Branch and Program Area

c) Name of Program or Service Representative

d) Key Program or Service Dates

This may include program or service initiation date, implementation date(s), project completion date, and other key milestones, if applicable.

2. Description

a) Summary of the New Program or Service or Change

i. General Description

Provide a brief explanation of the new program or service or change and include a brief explanation of the existing program, service or change.

ii. Purposes, Goals and Objectives

What are you trying to accomplish with this new program or service or change? For example:

- ✓ improving client services
- ✓ making program more efficient, saving on time and other resources
- ✓ improving protection of privacy
- ✓ standardization of a program component
- ✓ tracking incidence of a specific event
- ✓ obtaining sufficient information to administer the program

iii. The Need

Why are you making this new program or service or change?
Is it required by law, policy or standards?
Is it to fulfill a governmental/departmental commitment or mandate?

b) The Intended Scope

Outline both the planned and anticipated scope of the program or service. The "scope" may include:

- ✓ Conversion from a paper based information system to an electronic information system.
- ✓ Who is able to use the system? (e.g. in the current plan, only Department of XXX staff will have access to the system. In future it is anticipated that other Departments will have access). Note that the identification of specific users (e.g. clerks) will be covered in question 3 (g).
- ✓ Linkages with other systems or programs (e.g. an example of anticipated linkage is a plan to "link data collection system X with billing system Y by 2007").
- ✓ The type of information collected (e.g. in the first year the system will collect only name, address and contact information; by year three the system will include additional identifiable financial information).
- ✓ Future enhancements to the system (e.g. remote access).

- ✓ Future uses of the information (e.g. secondary use of data research or analysis).

c) Conceptual Technical Architecture (if applicable)

- ✓ Identify and describe the types of applications, platforms, and external entities involved in the information flow. Describe their interfaces, services, and the context within which the entities interoperate.
- ✓ This document is not intended to assess the technical security aspects of an electronic system. This section should be brief and clear to all readers. It is not intended to be or to replace a Threat Risk Assessment if one is required.

d) Description of Information Flow (include text and diagram to describe flow as necessary)

This section should include a diagram, but also requires a written description of any manual procedures and an identification of the staff who will be users of the system or who will receive information from the system.

3. Collection, Use and Disclosure of Personal Information

NOTE: Tables would be helpful to organize the answers to (a), (b), (c), and (d)

a) Authority for the Collection, Use and Disclosure of Personal Information

- ✓ Is there a law, regulation or authorized policy that allows you to **collect** the personal information as outlined in the new service or program or change?
- ✓ Is there a law, regulation or authorized policy that allows you to **use** the personal information as outlined in the new program or service or change?
- ✓ Is there a law, regulation or authorized policy that allows you to **disclose** the personal information as outlined in the new program or service or change?

b) List of Personal Information to be Collected, Used and/or Disclosed, the Method of Collection and Disclosure, and the Rationale for each.

There must be a reason or intended use for each item of personal information.

- ✓ List each item or field to be collected, and the reason or intended use for the collection.

For example:

Telephone number: To contact clients to update them on program changes
Financial information: To verify income

In general, good privacy principles mandate that the minimum amount of information necessary for the purpose is collected, used and disclosed. Is it necessary to collect each item of personal information to fulfill your purposes?

For example: do you need date of birth or would month and year of birth or age in years be sufficient?

In some cases it may be necessary to include information which may not appear to the writer to be “personal information”. This can be discussed with the reader; there may be information that in combination with other information would be categorized as “personal information”.

Do not exclude data elements on the basis that you think there are no privacy issues with the data elements. The data, in combination with other data held on this system or others may raise privacy issues.

Example of a table for this section:

Data Element	**Rationale for Collection, Use and/or Disclosure**	**Method of Collection and Disclosure**	**Comments**
Name	Collected to identify clients	Provided by client on application form Disclosed by email to approved vendors	

c) The Sources and Accuracy of the Personal Information

- ✓ Who is providing the information – the individual or another source (e.g. another government department, a family member)?
- ✓ Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed?
- ✓ Are there any data quality issues that are linked to user and system performance?

d) The Location of the Personal Information

- ✓ Is the information on servers or in a data repository? Will it be recorded on paper only and maintained in files?
- ✓ Where will the information be located? List all locations
- ✓ Will the information be stored in multiple locations? For example, will users be permitted to store information on other devices (e.g. laptops) or produce information from system (e.g. print and store in files)? If “Yes”, do you have a policy on protection of information held on electronic devices?
- ✓ Will the data be interfaced with data from other systems?
- ✓ If there is a data repository, give the name, description and geographical location of the repository.

e) The Retention Schedule and Method of Destruction or De-identification for Personal Information

- ✓ Is this information currently addressed in the Classification and Retention Schedule or is there a timetable for keeping the information in its identifiable form?
- ✓ Is retention monitored for compliance to the schedule?
- ✓ What is the plan and method of destruction (if any)?

f) Identification of Consent Issues

- ✓ Are you required by law, regulation or policy to obtain consent for the collection, use or disclosure of personal information?

For example:

- ✓ Sections 29, 31, 32 of MFIPPA outline the circumstances under which a municipality body may use and disclose personal information with and without consent.
- ✓ Do any of these sections apply?
- ✓ Please note that consent is not always required for collection, use and disclosure. It is important for you to confirm whether or not consent is required.
- ✓ Has the individual consented to the collection, use and disclosure anticipated in the new program or service or change? If yes, what is the method of requesting consent? Attach any consent form(s), and outline the process for obtaining consent.
- ✓ If consent has not been collected, have the subject individuals been notified (either specifically or generally) of the new program or service or change?

g) Users of Personal Information

- ✓ List the users (positions, not names) who will have access to the information.
- ✓ Describe the level of access each user group will have to personal information
- ✓ Include a brief rationale for each user's need to access the information.

A table would be very helpful for completion of this section:

User Group	Level of Access	Rationale	Comments
Clerical Staff	Demographic information only (Name, Address)	To address Letters and forms to clients	

4. Access Rights for Individuals to their Personal Information

Will individuals have access to their personal information on the system?

Note: MFIPPA gives individuals the rights of access to their own personal information with certain restrictions.

If yes:

- ✓ Describe your process for allowing individuals access to their personal information; and
- ✓ Indicate if individuals will be informed of the following: the information source(s) of their personal information?
- ✓ The uses and disclosures of their personal information? (see notice of collection template)

5. Privacy Standards: Concerns and Security Measures

a) Security Safeguards

Administrative Safeguards

- ✓ Do contracts with external service providers contain privacy provisions, which meet or exceed the privacy standards of the Municipal Freedom of Information and Protection of Privacy Act?
- ✓ Has staff received training on privacy and confidentiality policies and practices?
- ✓ Is access to the personal information restricted on a "need to know" basis? How is this determined?
- ✓ What controls are in place to prevent and monitor misuse of the personal information)?
- ✓ Is there a process in place for access or role changes for system users (e.g. users who leave employment or change jobs)?
- ✓ Describe the process in case of a breach of privacy.

Basic Technical Safeguards

Note: This section is intended to capture information related to basic technical safeguards (e.g. passwords, security related to the location of the information (e.g. locked filing cabinets). It is not intended to capture and assess the security elements of an information system which would be more properly assessed in a Threat/Risk Assessment.

- ✓ How is the personal information collected and transferred from the individual to the system/program?
- ✓ For example: electronic, paper, fax, and courier
- ✓ If the information is transmitted in electronic format, is it being transmitted within a secured server, is it encrypted?
- ✓ Are all accesses to the system password protected?
- ✓ Are all users trained on good password practices?
- ✓ Is there an automatic prompt for users to change their passwords? If yes, how often are they asked to change the password?
- ✓ Is remote access to the information permitted? If yes, what is the method for access? Is the information secure on transfer?
- ✓ Will the system be tested to ensure privacy controls are functioning?
- ✓ Are fax machines located in a secure, private area?

- ✓ Are paper files secured in a locked area with controlled access?

Auditing

- ✓ Does the level of sensitivity of the information require that use of this system be audited? If “No”, why not?
- ✓ Does the system have the capability to audit access and/or view the system?
- ✓ What is the level of information that audit can produce (e.g. can it identify individual patients/clients, pieces of information etc. that the user viewed)?
- ✓ Does the audit always run, or is it a system that must be switched on and off?
- ✓ Is there a limit to the time audit information is kept?
- ✓ Will an auditing plan be developed?
- ✓ Are resources being committed to the auditing and follow-up function?

b) Avoidance of Unintentional Disclosure

- ✓ Is the information reviewed prior to disclosure to prevent unintentional disclosure of personal information?
- ✓ When statistical information about a small group of individuals is disclosed outside the Department, there is a risk that these individuals could be identified.
- ✓ As a general guideline, do not disclose statistical information about groups (cells) containing less than 5 individuals.
- ✓ Are small cell sizes (e.g. cells of less than five) disclosed?
- ✓ If small cell sizes are to be disclosed, what is the rationale for doing so?

6. Conclusions

a) An Assessment of the Impact on Privacy, Confidentiality and Security of Personal Information as a Result of the New Program or Service or Change

Assess the privacy, confidentiality and security impact on personal information as a result of: The new program or service; Changes to the current program or service; Or anticipated future changes to the program or service. Discuss both negative and positive impacts

b) Strategy for Mitigation of Privacy Risks

Outline any plans or proposals for reducing or eliminating any negative impacts on privacy.

c) Additional Comments

Make any additional comments related to the privacy impact(s).

Personal Information Bank Listing
Town of Newmarket

(To be completed in 2014)

Appendix B.iv of Protection of Personal **Information Policy CORP.1-08**

Newmarket

Appendix C - Privacy Audit Procedures
to
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

1. All privacy audits will be managed by the Town Clerk or designate. An audit may be conducted internally by town staff or through an outside consultant.
2. A privacy audit may consist of document reviews, software or hardware checks, site visits and/or inspections, interviews or surveys.
3. Prior to an audit staff will:
    - Define scope of audit and approach;
    - Identify stakeholders and their responsibilities;
    - Complete Audit Plan;
    - Develop audit criteria.
4. Notification will be provided to senior management prior to any site visits or inspections and will consist of the date and purpose of the visit or inspection. Communication to staff will be the responsibility of each department.
5. A public report will be provided to senior management on the results of the privacy audit. This report will present the results and recommendations.
    a) If necessary any detailed observations or concerns may be presented to senior management in a separate confidential report outlining specific solutions to any identified problems.

Appendix D - Privacy Breach / Complaint Procedures
To
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

1. All privacy breaches and privacy complaints will be immediately reported to the supervisor / manager.
2. The supervisor / manager will call the Town Clerk or designate to report the complaint or breach.
3. The supervisor / manager will send an email to the Town Clerk or designate and their Director outlining in detail the circumstances of the breach or complaint, identifying all staff involved, and the personal information at issue.
4. The Records and Projects Coordinator will contact the staff involved directly if necessary for any questions or follow-up required.
5. The Records and Projects Coordinator will send a notification to all affected parties of a privacy breach. The notification will:
    a. provide details of the extent of the breach and the specifics of the personal information at issue;
    b. advise of the steps that have been taken to address the breach, both immediate and long-term; and
    c. advise that the Information and Privacy Commissioner of Ontario has been contacted to ensure that all obligations under the Act are fulfilled.
6. The Records and Projects Coordinator will report all privacy breaches to the Information and Privacy Commissioner of Ontario and senior management.
7. All privacy complaints will be investigated and a report submitted to senior management. The report shall include:
    a. A description of the circumstances of the complaint and the personal information involved; and
    b. An analysis of the cause of the complaint, staff actions and procedures, and any recommended solutions.

Appendix E - Website Privacy Policy
to
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

The Town of Newmarket is committed to providing our residents with information and services in a manner that respects and protects their privacy. This page summarizes the privacy statement and practices applicable to the interactions with the Town of Newmarket website.

We do not automatically gather any personal information from you unless it is supplied voluntarily. Any personal information you do provide is managed according to the Municipal Freedom of Information and Protection of Privacy Act (Ontario). We do use software to gather and store certain information about your visit to our web-site. This information does not identify you personally. We collect information such as the Internet domain used, the date and time of your visit, the pages visited and if you were referred to our site from another web site. This information is used to help us make our site more useful to visitors. Vendors of products and/or services may choose to register with the Town online which requires provision of personnel information. The Town of Newmarket does not and will not sell, rent, disclose, distribute or otherwise disseminate any information collected.

This site uses session-based (temporary) cookies that are created when you visit our site and last only for the duration of your visit. These are then automatically deleted. This generic session information is collected in a non-identifiable form to provide us with statistical information on pages visited.

The Town of Newmarket takes every precaution to protect your personal information on our website. We protect your account information by requiring you to enter a unique Login ID and password each time you want to access your account information. Your password should never be shared with anyone.

The Town of Newmarket uses SSL encryption technology to protect personal information (eg. credit card numbers, etc.) during transmission. A security icon will appear in your browser window to indicate that you are using a secure site. If you have any questions or concerns about the security at our website, you can send an email to webmaster@newmarket.ca

The Town's website contains links to other sites. Please be aware that the Town of Newmarket is not responsible for the privacy practices of other sites. When you leave our site, we encourage you to read the privacy statement of each and every website that you visit before you provide any personal information. The Town's privacy statement applies solely to information collected on the Town's website.

If you have any questions or comments regarding this statement, please contact the Town Clerk, Town of Newmarket, 395 Mulock Dr., P.O. Box 328, Station Main, Newmarket, ON L3Y 4X7, telephone 905-895-5193, fax 905-953-5100.

Appendix F - Procedures for Staff Access to Human Resources Personal Information
Town of Newmarket
Protection of Personal Information Policy CORP.1-08

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.