COUNCIL POLICIES AND PROCEDURES

SECTION- I

ETHICS

SUBJECT: Privacy Policy

POLICY NUMBER: I-4

APPROVAL DATE: June 20, 2018

PREAMBLE

The Municipality of the District of Guysborough (MODG) is committed to respecting the privacy rights of all individuals whose personal information it has collected and to ensuring the confidentiality and security of that personal information and to excellence in the management of that personal information. MODG will ensure adherence to the privacy protection provisions of Part XX (Freedom of Information & Protection of Privacy) of the Municipal Government Act (MGA), the Personal Information International Disclosure Protection Act (PIIDPA) and other applicable legislation. Violations of this policy whether intentional or inadvertent, may result in disciplinary action up to and including termination of employment. Where appropriate, legal sanctions may be pursued.

DEFINITIONS

Employee includes a person retained under an employment contract to perform services for MODG. For the purpose of this policy, an employee also includes individuals seconded to MODG and volunteers, students and interns who have access to records

FOIPOP Freedom of Information and Protection of Privacy, Part XX of the Municipal Government Act

Personal Information Personal information is recorded information about an identifiable individual including**:**

- the individual's name, address or telephone number;
- the individual's age, sex, sexual orientation, marital status or family status;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations
- an identifying employee number assigned to the individual;
- information about the individual's health-care history, including a physical or mental disability included in their personnel file
- information about the individual's educational, financial, criminal or employment history;

● anyone else's opinions about the individual; and
● the individual's personal views or opinions, except if they are about someone else.

Privacy Breach the event of unauthorized collection, access, use, disclosure, storage or alteration of personal information.

Record record as defined in Part XX of the MGA, includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

POLICY OBJECTIVES

The objectives of this policy are:

1. To ensure MODG meets it legislated and regulatory responsibilities in the management of personal information;

2. To ensure consistency in practices and procedures in administering the legislated and regulatory responsibilities;

3. To ensure effective protection and management of personal information by identifying, assessing, monitoring and mitigating privacy risks in MODG programs and activities involving the collection, retention, use, disclosure, storage and disposition of personal information;

4. To ensure only the minimum amount of personal information required for a specific purpose is collected, used or retained; and

5. To ensure that appropriate consent is obtained and that systems used for storing personal data comply with legal and regulatory requirements.

POLICY DIRECTIVES

1. This privacy policy applies to all MODG Employees, Council, residents and all personal information in the custody and/or control of MODG.

2. This privacy policy will be posted on MODG's website.

3. All MODG employees will be advised of the privacy policy and privacy awareness training will be available and delivered to employees.

4. MODG will collect, access, store, use, and disclose personal information only where authorized by law or agreement.

5. MODG will make reasonable efforts to ensure that the individual understands the purpose for which the personal information is being collected and the need for the collection.

6. MODG will limit its collection of personal information to that which is required for its programs and services; reasons for collection of this information will be provided at the time that consent is sought. Where an Act, Regulation or Municipal By-law requires that information be provided, consent will not be required for the collection of that information.

7. MODG will use and disclose an individual's personal information only for the purpose for which it was collected, for a use consistent with that purpose, for other purposes for which consent has been obtained, or for other purposes required or permitted by law.

8. MODG is committed to protecting personal information through appropriate administrative, technical and physical security measures and safeguards, regardless of the format in which the personal information is held.

9. MODG will retain personal information in accordance with legislative requirements and will ensure that proper care is taken in the disposal of personal information.

10. MODG will make every reasonable effort to ensure its records of an individual's personal information are accurate and complete and will allow a person access to their own information to verify, update and correct it.

11. MODG will ensure that this policy is considered for all new and significantly amended programs or services that collect, use or disclose personal information.

12. MODG will establish a privacy breach/complaint protocol as per Appendix A.

13. Complaints or questions with respect to this policy may be directed to MODG's Information Officer

Accountability & Security

ROLES AND RESPONSIBILITIES

Employees – All MODG employees are required to know and understand their obligations under this policy. Employees are expected to respect the confidentiality of personal information and report any breaches of privacy to their immediate supervisor. Employees will make reasonable efforts to ensure personal information is protected.

Directors & Supervisors– along with the responsibilities noted above, Directors and Supervisors are required to ensure that their staff follow this policy and the applicable Acts.
Information Officer – will provide advice and guidance to Elected Officials, Senior Management, and employees with respect to the treatment of personal information within MODG and will monitor and report on MODG's compliance with this policy.

CAO – along with the responsibilities noted above, the CAO is responsible for the proper application of Part XX of the MGA, PIIDPA and other Acts or policies with respect to an individual's personal information.

Monitoring and Review
The Information Officer will be responsible for monitoring compliance with this policy.

_____
Warden Vernon Pitts

_____
Chief Administrative Officer
Barry Carroll

_____
Date

Appendix A
Privacy Breach/Complaint Procedure

A. Statement

The Municipality of the District of Guysborough, in accordance with section 483 and 485 of the MGA, has the responsibility to:

1) be accountable to the public for the Information it collects and manages; and

2) protect the privacy of each Individual whose information it holds, and to allow the individual access to that information.

B. Objectives

This procedure is intended to assist employees in their response to:

1) the discovery of a privacy breach or a disclosure of sensitive information; or

2) a complaint from an individual about an alleged privacy breach or breach of sensitive information.

C. Definitions

"Sensitive Information" means Information which, if disclosed, could result in harm, disruption of government affairs or other negative consequences but does not include personal information;

All other definitions take the same meanings as those set out In the MODG Privacy Policy.

D. Directive: Security Arrangements

MODG is responsible for protecting personal and sensitive information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or disposal.

E. Accountability

Employees are required to adhere to this procedure.

Employees who are involved in the engagement of external agents or contractors by MODG are required to advise these parties that any privacy breach or potential privacy breach of personal or sensitive information must be immediately reported to the Access & Privacy Officer.

Managers and supervisors are responsible for monitoring compliance with this procedure and should address comments or concerns to both their Director and the Access & Privacy Officer.

F. Procedures for Managing and Reporting a Privacy Breach

Step 1 - Identify the Privacy Breach and take immediate action to contain or remedy it.
Step 2 - Notify the appropriate people about the Privacy Breach
Step 3 - Manage the Privacy Breach
Step 4 - Investigate and document the Privacy Breach
Step 5 - Follow-up and Long Term Action

Step 1 - Identify the Privacy Breach and take Immediate Action to Contain or Remedy It.

The employee responsible for the privacy breach or the employee who discovers the privacy breach must identify what happened and make his or her best effort to contain, minimize and remedy the damage from the privacy breach. For example:

a) If an electronic data device, such as a laptop or smartphone, is lost or stolen the employee must notify the Director of IT who will notify the Access & Privacy Officer.

b) If a fax is sent to the wrong number, the employee must call the recipient and ask them to destroy the document and any copies that were made.

c) If an e-mail is sent to the wrong person, the employee must call the recipient and ask them to securely destroy any e-mail printouts that were made and delete the e-mail.

d) If an employee discovers that an unauthorized person has or may have access to a database or computer system, the employee must notify the Director of IT who can disable accounts or change passwords and Identification numbers.

e) Some circumstances may create the impression that a privacy breach has occurred. If an Employee is uncertain whether a privacy breach has occurred, they should contact the Access & Privacy Office for direction.

Step 2 - Notify the appropriate people about the Privacy Breach

The employee must report the incident as follows:

a) To the police if a theft or other crime has occurred (for example, an office break-In, laptop or smartphone stolen);

b) To the employee's immediate supervisor;

c) To the Access & Privacy Officer who will help manage the privacy breach; (employee will complete appropriate form and forward to the Access & Privacy Officer); and

d) To the Director of IT to have passwords reset or to have a lost or stolen device wiped if applicable.

Step 3 - Manage the Privacy Breach

The appropriate Director, is responsible for coordinating the response of the incident to the Access & Privacy Officer. After appropriate consultation, the Access & Privacy Officer will make recommendations to the Director as to notification to the individual(s) whose personal information was the subject of the breach.

Step 4 -Investigate and Document the Privacy Breach

The employee's immediate supervisor must:

• Complete form A-l at the end of this Appendix;
• Follow-up on the privacy breach, which may include documenting:
- Recovery of the record or data device
- Identification of any additional loss of Information

Step 5 - Follow-up and Long Term Action

The Access & Privacy Officer will review the circumstances of the privacy breach to determine if policies, procedures or work practices are adequate to protect personal and sensitive Information and to prevent future privacy breaches.

The Access & Privacy Officer, together with staff, will determine what recommendations, if any, will be made to the Department in regard to follow-up and long-term remedial action to prevent the privacy breach from occurring again. This determination includes considering whether the privacy breach protocol was followed and whether any new or amended policies, procedures or work practices are required or if any training is required to prevent reoccurrence of the privacy breach.

G. Privacy Complaint Procedure
Employees may receive a call, email or letter from a citizen or another employee complaining of an alleged privacy breach of that person's personal information or a breach of sensitive information. Getting as much detail as possible and notifying the right people is the key to handling this type of communication. The steps to receiving a complaint are as follows:

Step 1 - Receive and Document the Complaint
Step 2 - Notify the Appropriate People
Step 3- Complainant Communication
Step 4- Follow-up and Long Term Action

Step 1 - Receive and Document the Complaint

a) When a complaint is received by telephone or in person, discuss the details of the alleged privacy breach with the complainant and document what the complainant believes has happened. This is a critical step and must be completed in writing so that it can form part of MODG's recorded response to the complaint.

b) When a complaint is received by email or letter, or once the details given by phone or in person have been captured, the complaint should be forwarded to the employee's immediate supervisor and to the Access & Privacy Office for appropriate action.

Step 2 - Notify the Appropriate People

The employee should report the complaint to his or her immediate supervisor.

The Immediate supervisor should report the complaint to the Office of the Director who will notify the Access & Privacy Officer.

The appropriate Director, in consultation with the Access & Privacy Officer, Is responsible for coordinating the investigation of the reported incident. The Access & Privacy Officer Is responsible, after appropriate consultation with the Director, or their designate, to make recommendations to the Department and to notify the CAO of the privacy breach if the Access & Privacy Officer considers It appropriate.

Step 3- Complainant Communication

Communication with the complainant will be done by the Access & Privacy Office and will consist of the following:

a) A written acknowledgement to the complainant, restating the details presented by the complainant and indicating MODG will be performing an investigation;

b) A written report updating the progress of the investigation (stage of investigation, follow-up activities, expected time frames) after no more than 60 calendar days has elapsed since the initial acknowledgement; and

c) A report of the results of the investigation - where a breach has been verified, the report will include a description of mitigating activities and any other follow-up activities.

Step 4- Follow-up and Long Term Action

The Access & Privacy Officer will review the circumstances of the privacy breach to determine if policies, procedures or work practices are adequate to protect personal and sensitive information and to prevent future privacy breaches.

The Access & Privacy Officer after consultation with staff, will determine what recommendations, if *any,* will be made to the Department with regard to follow-up and long-term remedial action to prevent the privacy breach from occurring again. This determination will consider whether the privacy breach protocol was followed and whether any new or amended policies, procedures or work practices are required or if any training is required to prevent recurrence of the privacy breach.

APPENDIX B
PRIVACY BREACH REPORTING FORM

If you are aware of a privacy breach that involves your Department, complete all sections of this form and submit it to the Access & Privacy Office. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer. A privacy breach occurs when there is unauthorized collection, access, use, disclosure, storage, disposition or alteration of **personal** Information in contravention of Part XX of the Municipal Government Act (For definition of personal information, see Privacy Policy)

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, for example a laptop containing personal information is stolen or a document with client information is e-mailed to the wrong person.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to the Access & Privacy Office.

CONTACT INFORMATION

Municipal Unit _____

Department _____

Contact:

Name: _____ Title: _____

Address:

_____

_____

_____

Phone: _____ Email: _____

Fax: _____

Date of Submission to the Access & Privacy Office:_____

** Please Indicate the date the Privacy Breach Reporting form is completed, not the date on which the privacy breach occurred.

Risk Evaluation

INCIDENT DESCRIPTION

1. Date the breach occurred: _____

2. Date the breach was discovered: _____

3. Describe the breach (provide sufficient detail, including cause):

_____
_____
_____
_____
_____
_____

4. Location of the breach (include civic address):

_____
_____
_____

5. Estimated number of individuals directly affected by the privacy breach *(i.e.* whose personal information has been compromised):

_____
_____

6. Type(s) of individuals affected (check all that apply):

_____ Client / Customer
_____ Employee
_____ Other (Please specify):

_____
_____
_____

7. Describe any immediate steps taken to reduce the harm of the breach *(e.g.* retrieval of breached information; replacement of locks; shut down of IT systems, etc.):

_____
_____
_____
_____
_____
_____
_____
_____

PERSONAL INFORMATION INVOLVED

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information.**

_____
_____
_____
_____
_____

SAFEGUARDS

9. If applicable, describe the **physical** safeguards *(e.g.* locks, alarm systems, etc.) used to protect this personal information:

_____
_____
_____
_____
_____

10. If applicable, describe the **administrative** safeguards (policies, procedures, etc.) currently in place to protect this personal information:

_____
_____
_____
_____
_____

11. If applicable, describe the **technical** safeguards (access controls, audit controls, etc.) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (Please specify):

_____
_____
_____

POTENTIAL HARM

12. Identify any potential damage, harm or injury that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)

• Physical harm or harassment *(e.g.* stalking)
• Emotional harm, humiliation or damage to reputation *(ex.* disclosure of personnel or health records)
• Financial cost
• Loss of business or employment opportunities
• Breach of contract and/or other legal obligations *(e.g.* from data loss)
• Future breaches (technical failures)
• Violation of professional standards or certificate standards
• Risk to public health or safety
• All of the above
• Other (Please specify):

NOTIFICATION

13. Have law enforcement officials been notified?

Yes. Who was notified and when?

_____
_____
_____

No. Will law enforcement be notified at a later time?

_____
_____
_____

14. Have you contacted legal services to discuss contractual and/or other legal obligations?

Yes. Who was notified and when?

_____
_____
_____

No

_____
_____

Completed by:_____ Date:_____

Supervisor/Manager: _____Date:_____

For Internal Use by the Access & Privacy Office only

Date Reporting Form received by the Access & Privacy Office:_____

Notes for Discussion:

Follow-Up:

Date Closed: _____

Signature of Access & Privacy Officer: _____