Privacy Management Program

PURPOSE

This program establishes the Municipal District of Provost No. 52's ("the M.D.") privacy obligations for the collection, use, disclosure, access, storage, retention, and disposal of Personal Information, as required by Section 25 of the Protection of Privacy Act (POPA).

SCOPE

This program applies to all M.D. of Provost employees, agents, volunteers, service providers, and elected officials.

This program does not apply to other Public Bodies differentiated from the M.D. of Provost by other governing legislation.

DEFINITIONS

Agent is an entity authorized to act for or in place of another.

Automated System is any system, software or process that uses computation as a whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities.

Artificial Intelligence System (AI) is a machine-based program that, for explicit or implicit objectives, infers from the input it receives how to generate outputs that can influence physical or virtual environments.

Contact Information is information to enable an individual or business to be contacted and includes the name, position or title, telephone number, address, email, or fax number of the individual or business.

Control is the power or authority to manage a Record throughout its life cycle, including restricting, regulating, and administering its use or disclosure.

Custody is having physical possession of a Record in addition to some right to deal with the Record and some responsibility for its care and protection. Custody normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security of the Record.

Data Matching refers to the linking of personal information between two or more databases or the electronic sources of information.

Information Sharing Agreement (ISA) is an agreement between a Public Body and at least one other Public Body or entity that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.

Non-Personal Data refers to data, including data derived from personal information, that has been generate, modified or anonymized so that it does not identify any individual.

Personal Information is recorded information about an identifiable individual other that Contact Information.

Personal Information Bank (PIB) is a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Privacy Breach means the theft or loss, or the collection, use or disclosure that is not authorized by POPA, of personal information in the Custody or under the Control of a Public Body.

Privacy Complaints are concerns raised by members of the public, organizations, M.D. employees or agents in relation to the M.D.'s handling of their Personal Information.

Privacy Impact Assessment (PIA) is a mandatory assessment that is conducted by a Public Body to determine if a current or proposed enactment, project, program or activity that involves personal information meets or will meet the privacy requirements of POPA.

Privacy Incident includes any event that has or could result in the theft or loss or the unauthorized collection, use, or disclosure of Personal Information.

Privacy Incident Response is a program control document that outlines steps in managing a known or suspected privacy breach.

Privacy Officer is the person designated within this program to ensure and maintain the municipality's compliance with POPA.

Public Body as described in Section 1 (t) in the ATIA, including Local Public Bodies (as defined in Section 1 (n) of the ATIA).

Records are 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 (as defined in Section 1 (u) of the ATIA).

Sensitive Personal Information is personal information with a higher risk of harm to individuals if the information is improperly collected, used or disclosed and may impact an individual's personal safety.

POLICY STATEMENTS

1. COMPLIANCE WITH POPA

All persons affiliated with the Municipal District of Provost No. 52, including employees, agents, volunteers, service providers, and elected officials, shall comply with all duties and obligations set out in POPA. This policy is intended to ensure compliance with POPA. To the extent that any portion of this policy conflicts, or can be interpreted to conflict with any provision of POPA, the provision of POPA will apply unless expressly set out herein.

2. ACCOUNTABILITY

2.1. Administrator

The Administrator is delegated as the Privacy Officer for the purpose of the M.D.'s statutory responsibilities under POPA. The Privacy Officer is authorized to delegate any or all of their POPA responsibilities to any other M.D. employee or agent. These responsibilities include:

- Developing, implementing and maintaining the M.D.'s Privacy Management Policy;
- Investigating and responding to Privacy Complaints and Privacy Incidents as per the privacy protocol;
- Completing or assisting employees with completing Privacy Impact Assessments;
- Providing privacy training to employees;
- Providing advisory services to employees;
- Maintaining the M.D.'s Personal Information Bank;
- Recommending remedial action in response to a breach of this policy or POPA;
- Representing the M.D. before the Office of the Information and Privacy Commissioner;
- Any other activity required under either POPA or ATIA
- Delegating duties assigned under this policy; and
- Participate in privacy training, as required.

2.2. Department Head

All Department Heads are responsible for:

- Complying with the privacy protection requirements in POPA and this policy;

- Communicating the requirements of POPA and this policy to employees in their department;
- Ensuring that Personal Information in the Custody and Control of their department is handled in accordance with POPA and this policy;
- Conducting and completing Privacy Impact Assessments prior to implementing new initiatives or significantly changing existing initiatives that involve Personal Information
- Establishing Information Sharing Agreements, as required; and
- Participate in privacy training, as required.

2.3. Employees/Volunteers/Agents

All employees, agents, elected officials, and volunteers are responsible for:

- Complying with the privacy protection requirements in POPA and this policy;
- Consulting with their Department Head and or the Privacy Officer regarding the requirements in POPA and this policy;
- Reporting Privacy Incidents to their supervisors and the Privacy Officer;
- Following instructions outlined by the Privacy Officer and/or delegate regarding privacy protection; and
- Participating in privacy training, as required.

2.4. Service Providers

The M.D. requires all third-party service providers, whose work on behalf of the M.D. involves the collection, use, access, disclosure, storage, retention or destruction of Personal Information, to abide by this policy and POPA.

3. TRAINING

All employees of the M.D. will be required to receive mandatory training with regards to this policy and the M.D.'s obligations under POPA upon the implementation of this policy.

Should any changes or updates be made to the M.D.'s obligations under this policy or POPA, employees will be required to be retrained regarding the changes to the policy.

4. COLLECTION

The M.D. must have legal authority to collect Personal Information. Collection must only occur as permitted under POPA.

Only the minimum amount of Personal Information will be collected to perform required M.D. functions.

Unless otherwise permitted by POPA, Personal Information will only be collected directly from the individual who the Personal Information is about.

5. NOTICE OF COLLECTION, PURPOSE, AND CONSENT

Personal information collected by the M.D. must only be collected for an identified M.D. program or activity.

Unless indirect collection is authorized under POPA, an individual from whom Personal Information is collected must be informed of the following:

- The purpose for collection of Personal Information;
- The legal authority for collecting Personal Information; and
- The title and Contact Information of an employee who can answer an individual's questions about the collection of Personal Information.

When the personal information is intended to be used in an automated system or AI to generate content or make decisions, recommendations or predictions, notice will be given at the time of collection.

Where necessary, informed consent for collection and use of Personal Information will be obtained prior to its collection.

6. USE, DISCLOSURE, AND ACCESS

Personal Information shall only be used, disclosed, or accessed:

- For the purpose for which it was collected;
- For a use that is consistent with the purpose for which it was collected;
- With the consent of the individual the information is about; or
- When a specific use, access, or disclosure is authorized by legislation.

Personal Information is only to be used, disclosed, or accessed as is required for the purposes of fulfilling work-related duties at the M.D.

For regular, systematic sharing of Personal Information, ISA's may be required to establish sufficient parameters and security measures around external use and disclosure of M.D.-held Personal Information.

7. ACCESS, ACCURACY, AND CORRECTION OF PERSONAL INFORMATION

If Personal Information is used by or on behalf of the M.D. to make a decision about an individual, the M.D. must make every reasonable effort to ensure that the Personal Information is accurate and complete.

Except in limited circumstances, individuals have the right to access their own Personal Information upon request.

Individuals have the right to request a correction of their factual Personal Information. A request for correction must be made by the person the information is about, unless otherwise permitted under POPA. This request may be made in person or via phone communication. A notation must be placed in the documentation if a correction cannot be applied. The individual must be advised of the reason their request was not applied.

8. STORAGE AND ACCESS INSIDE AND OUTSIDE OF CANADA

The M.D. must make every reasonable effort to ensure Personal Information in the Custody and Control of the M.D. is stored and/or accessed in Canada.

If Personal Information in the Custody and Control of the M.D. is to be stored and/or accessed outside of Canada a PIA must be completed and included in a supplemental assessment and approved by the Privacy Officer.

9. SECURITY CLASSIFICATION SYSTEM

All information held within the custody of the M.D. will be assigned a level within the Security Classification System. The level assigned to the various types of personal information within the Custody and Control of the M.D. will reflect the sensitivity of the personal information and the protocols regarding access to the associated information.

The M.D. will classify personal information using the following classification system:

SECURITY CLASSIFICATION LEVEL	ACCESS	HARM CAUSED TO INDIVIDUAL	EXAMPLE
PUBLIC	Unrestricted Access	No Harm	Public facing documentation/landowner names
INTERNAL	Employee Access	May Cause Limited Harm	Landowner mailing and contact information
CONFIDENTIAL	Authorized Personnel Access	May Cause Significant Harm	Tax/Arrears information

RESTRICTED	Specified Personnel Access	May Cause Serious Harm	Banking Information/Performance Evaluations

10. SECURITY AND PROTECTION

The M.D. will employ reasonable safeguards to prevent the unauthorized collection, use, access, disclosure, storage, or disposal of Personal Information. Security arrangements will include appropriate technological, physical, and administrative safeguards.

11. RETENTION AND DISPOSAL

The M.D. will retain an individual's Personal Information for at least one year when it is used to make a decision that directly affects an individual.

The M.D. will retain and dispose of Personal Information in accordance with the M.D.'s Records Retention Bylaw.

12. OPENNESS

This program will be made available to the public upon request within 30 days.

13. PRIVACY IMPACT ASSESSMENTS

The M.D. is required to prepare a privacy impact assessment ("PIA") under certain circumstances as per Section 26 of POPA with respect to a new, or substantial change to an existing, administrative practice, program, project, or service that will involve the collection, use or disclosure of personal information.

A PIA must provide a level of detail that that considers the complexity of the practice, program, project or service the PIA relates to. If a substantial change to an existing administrative practice, program, project, or service and there is already an associated PIA, the existing PIA may be amended to account for the change.

The Privacy Impact Assessments will be completed as per the requirements set forth in POPA and when required a completed copy will be forwarded to the Privacy Commissioner. In addition, the Information and Privacy Commissioner may also request a copy of a PIA under Section 27 of POPA.

14. CREATION, USE AND DISCLOSURE OF NON-PERSONAL DATA

The M.D. is authorized under Section 21 of POPA to create non-personal data for one or more of the following purposes:

- Research and analysis,
- Planning, administering, delivering, managing, monitoring or evaluating a program or service or;
- One or more other prescribed purpose that is allowed through regulation.

A quality assurance process will be utilized during the creation of non-personal data to:

- Verify and review the effectiveness of any methods used to create non-personal data,
- Ensure methods used to create the non-personal data can be replicated for auditing purposes,
- Identify and account for potential bias in the data, and;
- Ensure the accuracy and completeness of the non-personal data.

When creating non-personal data, the M.D. will only use personal information or data derived from personal information that is already in the custody and under the control of the M.D. Non-personal data will be created in accordance with generally accepted best practices and the prescribed requirements and regulations. The M.D. will use appropriate measure to ensure that the personal information or data that is used to create non-personal data is protected and a record regarding the creation and protection of the personal information used will be maintained in accordance with any prescribed requirements.

Upon the creation of non-personal data, the M.D. authorized to use this data for any purpose. However, before the non-personal information can be disclosed M.D. must complete an assessment that ensures, to the extent possible, that the identity of any individual who is the subject of the non-personal data cannot be identified or reidentified from the data, that identifies the security classification level of the created data, and identifies the risk level of reidentification and security measures taken to reduce the risk of reidentification.

The M.D. is authorized under Section 23 of POPA to disclose non-personal data with another public body. The M.D. will follow all regulations regarding the purpose of disclosure and conditions of disclosure when disclosing non-personal data to a person or organization that is not a public body.

15. DATA MATCHING AND DATA DERIVED FROM PERSONAL INFORMATION

The M.D. will only participate in data matching as per the circumstances set forth in Section 17 (1) of POPA. If the authority does not exist under this provision, then the M.D. will not utilize data matching to create data derived from personal information.

The M.D. will not collect information from individuals for the purpose of data matching. The M.D. will only conduct data matching using information that is obtained from another public body or information that is already within the custody and control of the M.D.

Should the M.D. intend to engage in data matching with one or more other public bodies, a PIA will be required and is required to be submitted to the Office of the Information and Privacy Commissioner.

Data derived from personal information may only be shared with another public body who provided the personal information for the purpose of data matching for the purpose initially intended. The M.D. must protect data derived from personal information through reasonable security arrangements.

The M.D. will either destroy any data derived from personal information or transform this information into non-personal data once the original purpose of the data has been fulfilled.

16. AUTOMATED SYSTEMS AND A.I.

Should the M.D. intend for personal information to be utilized by automated systems and/or AI, the individual the information is being collected from must be notified of this intended use at the time of collection.

Should the M.D. intend to utilize automated systems or AI to generate content or make decisions, recommendations or predictions regarding the services and programming offered within the M.D., the M.D. will adhere to all legislated obligations and ensure the principals of transparency, security, privacy, ethics and human control are maintained.

17. BREACHES OF POPA AND PRIVACY OFFENSES

If Personal Information or Sensitive Information in the Custody or Control of the M.D. is collected, used, or disclosed in a manner that is not authorized by POPA, a Privacy Breach will occur. A Privacy Breach under POPA will also constitute a breach in this policy.

All Privacy Incident must be reported to the Privacy Officer immediately upon discovery. In accordance with the Privacy Incident Response, the Privacy Officer and/or their delegate will lead an investigation to confirm if a Privacy Breach has occurred.

If a Privacy Incident occurs in which a reasonable person would consider there could be a real risk of significant harm to an individual as a result of the incident, the M.D. is required to provide written notice of the incident, without unreasonable delay, to the individuals whom there exists a real risk of significant harm, the Information and Privacy Commissioner and the Minister responsible for POPA.

Under POPA, the following actions are deemed offences:

- The wilful, unauthorized collection, use, or disclosure of Personal Information in a manner not authorize by POPA; and
- The wilful failure to notify the Privacy Officer of an unauthorized disclosure of Personal Information.

18. COMPLAINTS, INVESTIGATIONS AND BREACH OF POLICY

Complaints and suspected breaches of this program, and of POPA, should be addressed to the Privacy Officer who will give notice of the compliant to the Department Head of the applicable department. The M.D. is not required to respond to complaints, however, should the M.D. choose to respond to a complaint a response must be provided to the complainant within 30 days of the receipt of the complainant.

Upon notification, the Privacy Officer, or their delegate, will the initiate the Privacy Incident Response to determine if a Privacy Incident occurred. The Privacy Officer, or their delegate, may carry out an investigation and may use and disclose personal information contained in the complaint to employees or service providers of the M.D. as necessary for the purposes of conducting the investigation.

After the investigation, a written report will be prepared. The report may contain findings of fact and recommendations aimed at ensuring compliance with this policy and POPA.

If required, a copy of the report may be shared on a need-to-know basis to those involved in the investigation.

Breach of this policy, or of any procedure created or pursuant to it, or of POPA may be handled in accordance with the Personnel Policy.

Privacy Complaints/Incidents that may result in privacy offenses will be pursued in accordance with POPA.

Should the M.D. choose not to respond to a privacy complaint or the complainant is dissatisfied with the response and investigation completed by the M.D., the complainant may request a review be conducted by the Information and Privacy Commissioner under Section 37 of POPA.

19. PROGRAM REVIEW

This program will be reviewed on a yearly basis and updates will be completed as required.