POLICY

26 – 278 – 26/10/19
Department: Municipal Enforcement

PRIVACY

SCOPE

This policy applies to all personal information and records collected, created, accessed, used, disclosed, stored, retained, or disposed of by the Town of Nanton Municipal Enforcement Department in the performance of its duties.

This policy applies to all Municipal Enforcement Officers and includes information contained in enforcement files, notebooks, photographs, audio and video recordings, electronic records, correspondence, databases, and any other records created or accessed for municipal enforcement purposes.

Municipal Enforcement Officers shall comply with applicable federal and provincial privacy and access to information legislation, as amended from time to time, the requirements of the Peace Officer Program, and the Town of Nanton's Privacy Management Program and related policies and procedures.

OBJECTIVES

The purpose of this policy is to establish requirements for the protection of personal information collected, used, accessed, disclosed, stored, or otherwise managed by Municipal Enforcement and to ensure that personal information is handled only for authorized and lawful purposes.

This policy is intended to ensure Municipal Enforcement practices are consistent with the Town of Nanton's broader privacy, access to information, records management, information security, and privacy breach management requirements.

AUTHORITY

- Peace Officer Act
- Peace Officer Regulation
- Peace Officer (Ministerial) Regulation
- Access to Information Act
- Protection of Privacy Act
- Applicable federal and provincial privacy legislation, as amended from time to time
- Town of Nanton Privacy Management Program and related policies, procedures, standards, and bylaws

POLICY

1. Protection of Personal Information

1.1 Municipal Enforcement Officers shall protect personal information collected, created, accessed, used, disclosed, stored, or retained in the course of their duties from unauthorized access, use, disclosure, alteration, loss, or destruction.

1.2 Personal information shall only be collected where authorized by law and where reasonably necessary for a legitimate municipal enforcement purpose.

1.3 Municipal Enforcement Officers shall only access, use, or disclose personal information where required for the performance of their official duties and where authorized by applicable legislation or Town policy.

1.4 Municipal Enforcement Officers shall take reasonable steps to ensure personal information under their control is accurate, complete, secure, and protected against unauthorized access.

1.5 Personal information shall not be accessed, searched, used, copied, disclosed, or distributed for personal purposes or for any purpose unrelated to the Municipal Enforcement Officer's official duties.

2. Access to Information

2.1 Records created or maintained by Municipal Enforcement are subject to applicable access to information and privacy legislation.

2.2 Requests from members of the public for access to Municipal Enforcement records shall be referred to the Town employee responsible for administering access to information requests and shall be processed in accordance with the Town's established procedures.

2.3 A Municipal Enforcement Officer shall not independently release records in response to a formal access to information request unless authorized to do so.

2.4 Municipal Enforcement Officers shall cooperate with the Town in locating, retrieving, preserving, and reviewing records responsive to an access to information request.

2.5 Records subject to an access request, legal hold, investigation, complaint, or proceeding shall not be altered, deleted, or destroyed.

3. Use of Law Enforcement Databases

3.1 Municipal Enforcement Officers shall only access law enforcement or government databases for which they have been specifically authorized and trained.

3.2 This includes, where applicable, JOIN, ROADS, CPIC, motor vehicle databases, or any other law enforcement or government information system authorized for use by the Town of Nanton Municipal Enforcement Department.

3.3 Database access shall only be used for a legitimate and authorized law enforcement or municipal enforcement purpose directly related to the Municipal Enforcement Officer's official duties.

3.4 Municipal Enforcement Officers shall not access databases to obtain information about themselves, family members, friends, coworkers, acquaintances, public officials, or any other person unless the access is required for a legitimate and authorized enforcement purpose.

3.5 Usernames, passwords, access credentials, and other authentication information shall not be shared with another person.

3.6 Information obtained from an authorized database shall not be copied, retained, disclosed, or used except where necessary for the authorized purpose for which it was accessed and in accordance with applicable legislation and Town policy.

3.7 Municipal Enforcement Officers shall comply with all conditions, restrictions, security requirements, and user agreements established by the organization responsible for the applicable database.

3..8 Database access may be audited or reviewed to ensure compliance with applicable legislation, agreements, and Town policies.

4. Records and Information Security

4.1 Municipal Enforcement records containing personal information shall be stored only within Town-approved physical or electronic records systems.

4.2 Municipal Enforcement Officers shall take reasonable precautions to prevent unauthorized persons from viewing or accessing personal information, including information displayed on computer screens, mobile devices, notebooks, enforcement files, and other records.

4.3 Personal information shall not be stored on personal devices, personal email accounts, unauthorized cloud services, removable storage devices, or other systems not approved by the Town.

4.4 Physical records containing personal information shall be secured when not in use and shall not be left unattended in a location accessible to unauthorized persons.

4.5 Municipal Enforcement records shall be retained and securely disposed of in accordance with the Town of Nanton's Records Retention Bylaw and approved records management procedures.

5. Disclosure of Information

5.1. Personal information and Municipal Enforcement records shall only be disclosed where the disclosure is authorized or required by applicable legislation.

5.2. Except where disclosure is expressly authorized as part of the Municipal Enforcement Officer's regular enforcement duties or is required by law, the Municipal Enforcement Officer shall consult with the Town's designated Privacy Officer and/or Head before disclosing personal information or Municipal Enforcement records to another person, organization, or agency.

5.3. Information may be disclosed to the RCMP, Crown Prosecutors, other law enforcement agencies, government bodies, or other authorized persons where there is lawful authority for the disclosure and the disclosure is necessary for an authorized purpose.

5.4. Prior to disclosing personal information, the Municipal Enforcement Officer shall take reasonable steps to verify the identity and authority of the person requesting the information.

5.5. Disclosures of personal information shall be documented in accordance with the Town's Privacy Management Program and applicable procedures, including, where required, the information disclosed, recipient, date, purpose, and authority for the disclosure.

Privacy and Security Breaches

6.1 A Municipal Enforcement Officer who becomes aware of an actual or suspected loss, unauthorized access, collection, use, disclosure, alteration, or destruction of personal information shall immediately report the incident to the Town's Privacy Officer or Chief Administrative Officer (CAO).

6.2 The Municipal Enforcement Officer shall take reasonable and immediate steps, where safe and practicable, to contain the incident, preserve relevant records and evidence, and prevent any further unauthorized access, use, disclosure, loss, alteration, or destruction of information.

6.3 Privacy and security incidents shall be assessed and managed in consultation with the Privacy Officer or CAO and in accordance with the Town of Nanton's Privacy Breach Procedure, Incident Response and Third-Party Management Procedure, Privacy Management Program, and applicable legislation.

6.4 The Privacy Officer or CAO shall determine whether notification or reporting is required and ensure that any required notification is made to the appropriate authority, affected individual, law enforcement agency, database administrator, Peace Officer Program, or other organization in accordance with applicable legislation, agreements, policies, and procedures.

6.5 Where a privacy or security breach involves information obtained through JOIN, ROADS, CPIC, or another external database or information system, the incident shall also be reported through the applicable breach or incident reporting process required by the organization responsible for that system.

6.6 Municipal Enforcement Officers shall not independently notify affected individuals or external organizations of a privacy or security breach unless directed by the Privacy Officer or CAO, or where otherwise required by law.

6.7 Municipal Enforcement Officers shall cooperate fully with any investigation, assessment, containment, notification, remediation, or review arising from an actual or suspected privacy or security incident.

7. Confidentiality

7.1 Information obtained by a Municipal Enforcement Officer in the course of their duties shall be treated as confidential and shall only be discussed or shared where required for an authorized purpose.

7.2 Municipal Enforcement Officers shall not discuss confidential enforcement information in public areas or with persons who do not have an authorized need to know.

7.3 The duty to protect confidential and personal information continues after an Officer's employment or appointment with the Town of Nanton ends.

8. Compliance with Town Privacy Requirements

8.1 This policy shall be read in conjunction with the Town of Nanton's Privacy Management Program and all applicable privacy, access to information, records management, information security, and acceptable technology use policies and procedures.

8.2 Where the Town's corporate privacy or information security requirements establish a higher standard of protection than this policy, the higher standard shall apply unless otherwise prohibited by law or incompatible with a specific Peace Officer Program requirement.

8.3 Municipal Enforcement Officers shall complete any privacy, information security, records management, or database training required by the Town or the applicable system administrator.

9. Review and Audit

9.1 The Chief Administrative Officer may review Municipal Enforcement records, database access, information handling practices, and related documentation to verify compliance with this policy.

9.2 Any suspected inappropriate access, use, disclosure, or handling of personal information shall be reviewed and, where appropriate, investigated.

9.3 Municipal Enforcement Officers shall cooperate with any privacy audit, investigation, access review, or compliance review conducted or authorized by the Town.

10. Non-Compliance

10.1 Municipal Enforcement Officers are required to comply with this policy, applicable legislation, database access requirements, and the Town's Privacy Management Program and related policies and procedures.

10.2 Failure to comply with these requirements may result in review by the Chief Administrative Officer. Depending on the nature and severity of the non-compliance, corrective action may include:

a. coaching or verbal direction;
b. additional privacy, security, or database training;
c. restriction or suspension of access to Town or law enforcement information systems;
d. documented performance management;
e. disciplinary action in accordance with the Town of Nanton's Progressive Discipline Policy; and/or
f. any reporting or other action required by applicable legislation, the Peace Officer Program, or the organization responsible for an affected database.

10.3 Intentional or unauthorized access, use, disclosure, alteration, destruction, or misuse of personal information or law enforcement databases may constitute serious misconduct and may result in disciplinary action and any other action required or authorized by law.

AMENDMENTS / REVIEWS:

Date (yyyy/mm/dd)	Section # Amended	Comments

Next Review Date:	

MAYOR — Date: Oct. 19/26

CHIEF ADMINISTRATIVE OFFICER — Date: Oct. 19/26

Policy: 26 – 278 – 26/10/19
Previous: n/a