BLACKFALDS
ALBERTA

Town of Blackfalds

Privacy Management Program

Approved by the Chief Administrative Officer (CAO)

Effective June 11, 2026

Overview

The *Protection of Privacy Act* (POPA) stipulates that all public bodies in Alberta develop and implement a Privacy Management Program. This policy framework assists Town employees in handling personal information appropriately and limiting privacy risks.

Through this Program, the Town of Blackfalds is able to protect personal information, address risks, and comply with legislated requirements.

Privacy Management Structure

Privacy Officer Designation

In accordance with Section 6(1)(a) of Protection of Privacy Ministerial Regulation AR 143/2025, the Town has designated a Privacy Officer to ensure compliance with POPA.

Title:	Information Governance Coordinator
Department:	Information Technology
Email:	access@blackfalds.ca

The Privacy Officer is responsible for:

- Overseeing the Town's compliance with POPA and the Privacy Management Program;
- Providing advice to Town employees regarding privacy risk management and information security;
- Reviewing and approving privacy impact assessments;
- Managing privacy incident (breach) investigation and response;
- Ensuring all Town employees receive training pertaining to access and privacy;
- Liaising with the Office of the Information and Privacy Commissioner; and
- Reviewing, maintaining and updating the Privacy Management Program.

*** In the absence of the Information Governance Coordinator, the roles and responsibilities of the Privacy Officer will be fulfilled by the Senior Legislative Advisor.*

Review, Maintenance and Update

The Privacy Management Program is reviewed as required, but no less than every three years. Reviews and necessary updates are completed by the Privacy Officer.

Public Availability

This Privacy Management Program is available to the public, as mandated by Protection of Privacy Ministerial Regulation AR 143/2025.

Corrections and Complaints

Requests to Correct Personal Information

It is important that personal information held by the Town is complete and accurate. If you feel that your personal information is incorrect, you may ask for it to be revised by completing a Request to Correct Personal Information Form.

Requests for correction will be handled in accordance with Section 7 of the *Protection of Privacy Act*.

Complaint Response

In order to provide our programs and services, the Town must collect, use, and often disclose personal information. If you feel that your personal information has been handled inappropriately, you may register a complaint to the Town of Blackfalds by emailing access@blackfalds.ca.

We will acknowledge receipt of your complaint and respond no later than 30 business days after we receive it.

If we do not resolve your complaint satisfactorily, you may reach out to the Information and Privacy Commissioner to request a review of the matter.

Information Security and Safeguards

Security Classification

The Town maintains an information security classification system that applies to all personal information in the Town's custody or control. Designations include Public, Internal, Confidential and Restricted.

The Directory of Personal Information Banks outlines categories of personal information held by the Town, along with their assigned information security classification level(s).

Automated Systems and Safeguards

Often, provision of the Town's programs and/or services involves automated systems which hold/use personal information. The Automated Systems and Safeguards Procedure Matrix (Procedure Schedule A) outlines the systems in place, along with safeguards utilized to protect the information within. As permitted by Section 6(4) of Protection of Privacy Ministerial Regulation AR 143/2025, specific technical and security details have been omitted.

Employee Education

Mandatory Training

All Town employees receive training in regard to access and privacy.

New employees complete online training provided by the Government of Alberta within 30 days of hiring.

In-house access and privacy training is provided to all eligible employees every three years and records of completion are retained by Human Resources.

This training, in relation to POPA, addresses:

- Employee responsibilities under the Act;
- Rules for collection, use, and disclosure of personal information;
- The right to request correction of personal information;
- How to identify and respond to privacy incidents; and
- The Town's privacy management structure and key roles.

Risk Assessment and Consent

Privacy Impact Assessment (PIA)

The Town's Privacy Impact Assessment Policy and Procedure lay out when a privacy impact assessment must be completed, as well as the review and approval process.

Consent

The Town adheres to the provisions of Section 2 of Protection of Privacy Regulation AR 132/2025 when requesting consent for use or disclosure of personal information, as required.

Supporting Documents

- Access to Information Delegation Policy
- Delegation and Assignment of Responsibility
- Information Security Classification Policy
- Information Security Classification Procedure
- Protection of Privacy Complaint Handling Policy
- Protection of Privacy Complaint Handling Procedure
- Non-Personal Data Policy
- Non-Personal Data Procedure
- Consent Policy
- Consent Procedure
- Correction of Personal Information Policy
- Correction of Personal Information Procedure
- Privacy Impact Assessment Policy
- Privacy Impact Assessment Procedure
- Privacy Incident Policy
- Privacy Incident Procedure
- Automated Systems and Safeguards Policy
- Automated Systems and Safeguards Procedure

ACCESS TO INFORMATION DELEGATION

POLICY NO	AP-004.24
DIVISION DEPARTMENT	Administration/Information Technology/Legislative Services
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To outline the Delegation of roles, powers and responsibilities under the *Access to Information Act,* the *Protection of Privacy Act* and the Access to Information Bylaw.

2. POLICY STATEMENT

2.1 The Town of Blackfalds supports and upholds the rights of individuals to request access to information in its custody or control. These rights are effectively balanced with the privacy expectations of the community at large.

3. DEFINITIONS

3.1 "**Acts**" means the *Access to Information Act* and the *Protection of Privacy Act*.

3.2 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.3 **"Delegation**" means the formal process whereby the Head of a public body authorizes an employee or officer within the public body to perform certain duties or exercise certain powers or functions of the Head under the Acts.

3.4 "**Director**" means the Employees who are directly responsible for a specific division of the Town.

3.5 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee, but does not include an individual who is a member of a class of individuals excluded by regulations.

3.6 "**Head**" means the Chief Administrative Officer (CAO), who is responsible for the administration of the *Access to Information Act* and the *Protection of Privacy Act* at the Town of Blackfalds.

3.7 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.8 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.9 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to Town of Blackfalds Employees who are involved in the administration of the *Access to Information Act* and the *Protection of Privacy Act*.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Directors and Managers to:

5.1.1 Understand and adhere to this Policy.

5.1.2 Ensure implementation of this Policy.

5.2 Information Governance Coordinator to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.2.3 Make recommendations to the CAO of necessary Policy amendments.

5.2.4 Ensure this policy is reviewed every three years, or as otherwise required.

5.2.5 Carry out the duties, powers and responsibilities of the Head of the municipality that are delegated to the position by the Delegation and Assignment of Responsibility, *Access to Information Act*, and Access to Information Bylaw.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this policy is reviewed every three years, or as otherwise required.

5.4.3 In the absence of the Information Governance Coordinator, carry out the duties, powers, and responsibilities of the Head of the municipality that are delegated to the position by the Delegation and Assignment of Responsibility, *Access to Information Act*, and Access to Information Bylaw.

5.4.4 Understand and adhere to this Policy.

6 POLICY

6.1 In accordance with the Access to Information Bylaw and the attached Delegation and Assignment of Responsibility, the duties, powers and responsibilities of the Head of the municipality are delegated to the position of Information Governance Coordinator and, in their absence, to the position of Senior Legislative Advisor.

6.2 The Delegation under Section 6.1 is subject to the following stipulations:

a) that the individual to whom the duties, powers and responsibilities are delegated is bound by the same administrative, jurisdictional, and legislative limitations as the Head pursuant to the Acts, and the Access to Information Bylaw, and

b) that notwithstanding this Delegation, the authority to exercise any duty, power or responsibility under the Acts and the Access to Information Bylaw, at any time, is retained by the Head.

7 RELATED DOCUMENTS

7.1 *Access to Information Act*
7.2 *Protection of Privacy Act*
7.3 Access to Information Bylaw
7.4 Delegation and Assignment of Responsibility – Attached

8 END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

March 16, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
September 11, 2024	K. Isaak	CAO
March 16, 2026	K. Isaak	CAO

BLACKFALDS
ALBERTA

Access to Information Act & Protection of Privacy Act

Delegation and Assignment of Responsibility

Duty, Power, or Function of Head	Section Reference	Retained By Head	Delegated to IGC	Delegated to Other Person(s)
Right of Access				
Establish process for receiving access requests	ATIA, Sections 2(a), 2(b), 2(c)		X	
Assure process for access is made public	ATIA Regulation, Section 3(1)		X	
Authority to disregard requests	ATIA, Section 9(1)		X	
Authority to declare request abandoned	ATIA, Section 10(1)		X	
Authority to grant continuing request	ATIA, Section 11(2)		X	
Duty to assist applicants	ATIA, Section 12(1)		X	SLA
Duty to provide access to records	ATIA, Section 12(2)		X	SLA
Authority to decide on content of response, and grant or refuse access	ATIA, Sections 13, 14(1)		X	SLA
Authority to refuse to confirm or deny the existence of a record	ATIA, Section 14(2)		X	SLA
Authority to decide how access will be given	ATIA, Section 15		X	SLA
Authority to request Commissioner's permission for extension	14(1), 14(2)		X	SLA
Authority to extend time limit	14(1), 14(3)		X	SLA
Authority to transfer a request for access	ATIA, Section 17		X	
Authority to withhold information harmful to business interests of a third party	ATIA, Section 19		X	SLA
Authority to withhold information harmful to personal privacy	ATIA, Section 20		X	SLA
Authority to withhold information harmful to individual or public health or safety	ATIA, Section 21		X	SLA
Authority to withhold confidential evaluations	ATIA, Section 22		X	SLA
Authority to withhold information harmful to law enforcement	ATIA, Section 23		X	SLA
Authority to withhold information harmful to workplace investigations	ATIA, Section 24		X	SLA
Authority to withhold information about disclosures to the Labour Relations Board	ATIA, Section 25		X	SLA
Authority to withhold information harmful to intergovernmental relations	ATIA, Section 26		X	SLA
Authority to withhold Cabinet confidences	ATIA, Section 27		X	SLA
Authority to withhold local public body confidences	ATIA, Section 28		X	SLA
Authority to withhold advice from officials	ATIA, Section 29		X	SLA
Authority to withhold information harmful to economic interests of a public body	ATIA, Section 30		X	SLA
Authority to withhold testing procedures, tests, and audits	ATIA, Section 31		X	SLA
Authority to withhold privileged information	ATIA, Sections 32(1), 32(2)		X	SLA
Authority to withhold information harmful to conservation of heritage sites, etc.	ATIA, Section 33		X	SLA
Authority to withhold information that is or will be available to the public	ATIA, Section 34		X	SLA

IGC = Information Governance Coordinator
SLA = Senior Legislative Advisor

Duty, Power, or Function of Head	Section Reference	Retained By Head	Delegated to IGC	Delegated to Other Person(s)
Third Party Intervention				
Duty to give third party notice	ATIA, Section 35		X	SLA
Authority to decide whether to give access to third party information	ATIA, Section 36(1)		X	SLA
Public Interest				
Authority to disclose information in the public interest	ATIA, Section 37(1)	X		
Duty to give notice to third party and Privacy Commissioner	ATIA, Sections 37(3), 37(4)	X		
Collection, Correction, Protection of Personal Information				
Establish controls over the collection, use and disclosure of personal information	POPA, Sections 2(a), 2(c)		X	
Authorize routine correction of personal information	POPA, Section 2(b)		X	SLA
Ensure authorized purpose of collection	POPA, Section 4		X	SLA
Assure proper collection and notification	POPA, Section 5		X	SLA
Authority to set aside collection requirements	POPA, Section 5(3)		X	
Assure accuracy of personal information	POPA, Section 6(a)		X	SLA
Apply retention standards	POPA, Section 6(b)		X	
Authority to decide on requests for correction of personal information	POPA, Section 7(1)		X	
Duty to correct, annotate or link personal information, and duty to notify previous recipients	POPA, Sections 7(3), 7(4)		X	
Duty to give notice to individual requesting correction	POPA, Section 7(7)		X	
Authority to transfer a request for correction	POPA, Section 8		X	
Duty to ensure protection of personal information	POPA, Section 10		X	SLA
Use and Disclosure of Personal Information				
Establish rules for electronic consent	POPA Regulation, Section 2(5)(a)		X	
Establish rules for oral consent	POPA Regulation, Section 2(6)(a)		X	
Assure appropriate uses	POPA, Section 12		X	SLA
Assure proper disclosures of personal information	POPA, Section 13		X	SLA
Disclose if not an unreasonable invasion of third party's personal privacy	POPA, Section 13(1)(a)		X	SLA
Disclose for original or consistent purpose	POPA, Section 13(1)(b)		X	SLA
Disclose after individual consents	POPA, Section 13(1)(c)		X	SLA
Disclose to comply with enactment of Alberta or Canada or treaty, arrangement or agreement made under enactment	POPA, Section 13(1)(d)		X	SLA
Disclose in accordance with enactment of Alberta or Canada that authorizes or requires disclosure	POPA, Section 13(1)(e)		X	SLA
Disclose to comply with subpoena, warrant, or court order from court, person, or body with jurisdiction in Alberta	POPA, Section 13(1)(f)	X	X	SLA
Disclose where necessary for employee of public body or member of Executive Council to perform duties	POPA, Section 13(1)(g)		X	SLA
Disclose where necessary for delivery of common or integrated program or service	POPA, Section 13(1)(h)		X	SLA
Disclose to enforce legal right of Government of Alberta or public body	POPA, Section 13(1)(i)	X	X	SLA
Disclose to collect debt or fine or make payment	POPA, Section 13(1)(j)	X	X	SLA
Disclose to determine or verify eligibility for program or benefit	POPA, Section 13(1)(k)		X	SLA
Disclose to Auditor General and other prescribed persons for audit purposes	POPA, Section 13(1)(l)	X	X	SLA
Disclose to Member of Legislative Assembly to assist individual	POPA, Section 13(1)(m)	X	X	SLA

IGC = Information Governance Coordinator
SLA = Senior Legislative Advisor

Duty, Power, or Function of Head	Section Reference	Retained By Head	Delegated to IGC	Delegated to Other Person(s)
Disclose to bargaining agent on behalf of employee	POPA, Section 1340(1)(n)		X	SLA
Disclose for archival purposes	POPA, Section 13(1)(o)		X	SLA
Disclose to assist investigation	POPA, Section 13(1)(p)	X	X	SLA
Disclose to next of kin or friend of injured, ill, or deceased individual	POPA, Section 13(1)(r)	X	X	SLA
Authority to disclose to relative or adult interdependent partner of deceased individual	POPA, Section 13(1)(s)		X	SLA
Disclose in accordance with Section 15 or 16	POPA, Section 13(1)(t)		X	SLA
Disclose for legal proceedings to which the Government of Alberta or public body is a party	POPA, Section 13(1)(u)	X	X	SLA
Disclose to manage or administer personnel	POPA, Section 13(1)(w)	X	X	SLA
Disclose to enforce a maintenance order	POPA, Section 13(1)(x)		X	SLA
Disclose to an officer of the Legislature where necessary to carry out duties	POPA, Section 13(1)(y)	X	X	SLA
Disclose for supervision of individual under control of correctional authority	POPA, Section 13(1)(z)	X	X	SLA
Disclose to lawyer acting for an inmate	POPA, Section 13(1)(aa)	X	X	SLA
Disclose when information is available to the public	POPA, Section 13(1)(bb)		X	SLA
Authority to disclose to avert imminent danger to health or safety	POPA, Section 13(1)(cc)	X	X	SLA
Disclose to administrator of the *Motor Vehicle Claims Act*	POPA, Section 13(1)(dd)		X	SLA
Disclose for research and statistical purposes and for administration of research agreements	POPA, Section 15		X	SLA
Authority to approve conditions for disclosure for research and statistical purposes and for administration of research agreements	POPA, Section 15(c)		X	
Disclose information in archives	POPA, Section 16		X	SLA
Authority to ask the Privacy Commissioner for advice	POPA, Section 28(1)		X	SLA
Authority to disclose to guardian of a minor	POPA, Section 54(1)(e)	X	X	SLA
Authority to require Commissioner to examine original record on site	ATIA, Section 50(4)	X	X	
Right to make representations to the Privacy Commissioner	ATIA, Sections 62(6), 62(8), 62(9)		X	
Duty to discharge burden of proof	ATIA, Section 63		X	
Duty to comply with Commissioner's Order(s)	ATIA, Section 66		X	SLA
General Provisions				
Duty to publish a directory of the public body's personal information banks and keep it current	POPA, Sections 57(2), 57(5)		X	
Duty to record uses or disclosures of personal information not included in directory	POPA, Section 57(4)		X	
Authority to specify categories of records available without formal request and require a fee	ATIA, Section 90	X	X	
Duty to make manuals available	ATIA, Section 91	X	X	
Fees				
Authority to assess and collect fees	ATIA, Section 96		X	SLA
Authority to waive fees	ATIA, Section 96(5)	X	X	
Duty to give notice of decision to grant or refuse fee waiver request	ATIA, Section 96(6)	X	X	SLA

IGC = Information Governance Coordinator
SLA = Senior Legislative Advisor

INFORMATION SECURITY CLASSIFICATION

POLICY NO	AP-082.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To establish standards for the classification of Personal Information, Data Derived from Personal Information, and Non-Personal Data in the custody of the Town of Blackfalds.

2. POLICY STATEMENT

2.1 The Town of Blackfalds recognizes that information related to its residents and Employees varies greatly in sensitivity. The assignment of security Classification enables the Town to more easily identify categories of information and implement appropriate safeguards.

3. DEFINITIONS

3.1 "**Acts**" means the *Access to Information Act* and the *Protection of Privacy Act*.

3.2 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.3 "**Classification**" means the action or process of classifying something according to shared qualities or characteristics.

3.4 "**Data Derived from Personal Information**" means data created by Data Matching which identifies any individual whose Personal Information was used in the Data Matching.

3.5 "**Data Matching**" means linking Personal Information between two or more databases or other electronic sources of information.

3.6 "**Director**" means the Employees who are directly responsible for a specific division of the Town.

3.7 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee but does not include an individual who is a member of a class of individuals excluded by regulations.

3.8 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.9 "**Non-Personal Data**" means data, including Data Derived from Personal Information, that has been generated, modified, or anonymized so that it does not identify any individual.

3.10 "**Personal Information**" means recorded information about an identifiable individual including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.11 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Director and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years or as otherwise required.

5.5 All Employees to:

5.5.1 Understand and adhere to this Policy.

6. POLICY PARTICULARS

6.1 In accordance with *Protection of Privacy Ministerial Regulation AR 143/2025*, the Town of Blackfalds will develop and implement a system to assign security Classification levels to Personal Information, Data Derived from Personal Information and Non-Personal Data in its custody or control.

7. RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 *Protection of Privacy Ministerial Regulation AR 143/2025*
7.3 Information Security Classification – Administrative Procedure
7.4 Information Security Classification Grid - Attached
7.5 Directory of Personal Information Banks

8 END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

March 16, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
March 16, 2026	K. Isaak	CAO

INFORMATION SECURITY CLASSIFICATION

POLICY NO.	PR-022.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Access to Information Act*, the *Protection of Privacy Act*, and *Protection of Privacy Act Ministerial Regulation AR 143/2025*.

1.2 Failure to identify and adequately safeguard sensitive information may lead to breaches of personal privacy, potentially resulting in harm to individuals and/or the Town and impacting public trust.

1.3 All referenced definitions can be located in the governing Information Security Classification Administrative Policy.

2. GENERAL

2.1 Classification Levels

2.1.1 Classification levels assigned to Personal Information, Data Derived from Personal Information and Non-Personal Data will consist of the following designations, based on the sensitivity of the information:

a. Public
b. Internal
c. Confidential
d. Restricted

2.1.2 The Information Security Classification Grid provides definitions and examples for each of these designations.

2.2 Personal Information and Data Derived from Personal Information

2.2.1 Security classification(s) assigned to Personal Information and Data Derived from Personal Information will be established by Departments, in cooperation with the Information Governance Coordinator.

2.2.2 The Classification levels assigned to Personal Information and Data Derived from Personal Information will be logged, with the corresponding category of information, in the Town's Directory of Personal Information Banks.

2.2.3 Classification levels must reflect the sensitivity of the information.

2.3 Non-Personal Data

2.3.1 Security classification(s) assigned to Non-Personal Data will be established by Departments, in cooperation with the Information Governance Coordinator.

2.3.2 The Classification levels assigned to Non-Personal Data will appear in a footnote on relevant document(s).

2.3.3 Non-Personal Data may only be classified Public or Internal.

2.3.4 Town Employees may not, at any time, de-anonymize or otherwise modify Non-Personal Data in an attempt to identify the individual(s) the information is about.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak

Chief Administrative Officer

March 16, 2026

Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
March 16, 2026	K. Isaak	CAO

NON-PERSONAL DATA

POLICY NO	AP-085.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To guide Employees of the Town of Blackfalds in the creation, use and/or disclosure of Non-Personal Data.

2. POLICY STATEMENT

2.1 The Town of Blackfalds recognizes the potential value of using Non-Personal Data for research, analysis, and the identification of relationships, patterns and trends.

3. DEFINITIONS

3.1 "**Act**" means the *Protection of Privacy Act.*

3.2 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.3 "**Data Derived from Personal Information**" means data created by Data Matching which identifies any individual whose Personal Information was used in the Data Matching.

3.4 "**Data Matching**" means linking Personal Information between two or more databases or other electronic sources of information.

3.5 "**Director**" means the Employees who are directly responsible for a specific division of the Town.

3.6 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee, but does not include an individual who is a member of a class of individuals excluded by regulations.

3.7 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds.

3.8 "**Non-Personal Data**" means data, including Data Derived from Personal Information, that has been generated, modified, or anonymized so that it does not identify any individual.

3.9 "**Personal Information**" means recorded information about an identifiable individual including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.10 "**Privacy Management Program**" means a framework of Policies and Procedures that clearly demonstrate the Town's compliance with the Protection of Privacy Act.

3.11 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.12 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Director and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years or as otherwise required.

5.4 All Employees to:

5.4.1 Understand and adhere to this Policy.

6 POLICY PARTICULARS

6.1 In accordance with Division 2 of the *Protection of Privacy Act*, the Town of Blackfalds will develop and implement procedures for the creation, use and disclosure of Non-Personal Data.

7 RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 *Protection of Privacy Ministerial Regulation AR 143/2025*
7.3 Administrative Procedure - Non-Personal Data
7.4 Creation of Non-Personal Data Tracking Form
7.5 Non-Personal Data Agreement

8 END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

Apr 17, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
Apr 17, 2026	Kim Isaak	CAO

NON-PERSONAL DATA

POLICY NO.	PR-025.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act* and *Protection of Privacy Ministerial Regulation AR 143/2025.*

1.2 Section 6(1)(b)(ii) of *Protection of Privacy Ministerial Regulation AR 143/2025* mandates that the Town's Privacy Management Program must include Policies and Procedures for the creation, use and disclosure of Non-Personal Data.

1.3 Sections 21-24 of the *Protection of Privacy Act* govern the creation, use, disclosure and protection of Non-Personal Data.

1.4 All referenced definitions can be located in the governing Non-Personal Data Policy.

2. GENERAL

2.1 Creation of Non-Personal Data

2.1.1 The Town of Blackfalds may create Non-Personal Data, including Data Derived from Personal Information, only for the following purposes:

a. research and analysis;

b. planning, administering, delivering, managing, monitoring or evaluating a program or service.

2.1.2 Non-Personal Data must be created in accordance with generally accepted best practice.

2.1.3 In order to create Non-Personal Data, the Town may use Personal Information or Data Derived from Personal Information only if it is already in the Town's custody or under its control.

2.1.4 Every time the Town creates Non-Personal Data, it must be documented on a Creation of Non-Personal Data Tracking Form.

2.1.5 Completed forms must be forwarded to the Information Governance Coordinator for electronic filing and retention.

2.2 Use of Non-Personal Data

2.2.1 The Town may use Non-Personal Data it creates for any purpose.

2.3 Disclosure of Non-Personal Data to Other Public Bodies

2.3.1 The Town may disclose Non-Personal Data to another public body for any purpose.

2.4 Disclosure of Non-Personal Data to Individuals

2.4.1 The Town can disclose Non-Personal Data to any person only for the following purposes:

a. research and analysis;

b. planning, administering, delivering, managing, monitoring or evaluating a program or service.

2.4.2 The CAO must approve conditions relating to the following:

a. security and confidentiality;

b. the prohibition of any actual or attempted re-identification of the Non-Personal Data;

c. the prohibition of any subsequent use or disclosure of the Non-Personal Data without express authorization from the Town.

d. the destruction of the Non-Personal Data once it has served its purpose.

2.4.3 Individuals wishing to utilize the Town's Non-Personal Data must sign an agreement to comply with the approved conditions, the *Protection of Privacy Act*, and the Town's Policies and Procedures relating to Non-Personal Data.

2.5 Protection of Non-Personal Data

2.5.1 The Town must make reasonable security arrangements to guard against risks such as unauthorized access, collection, use, disclosure or destruction of its Non-Personal Data.

2.6 Re-Identification

2.6.1 Town Employees may not, at any time, de-anonymize or otherwise modify Non-Personal Data in an attempt to identify the individual(s) the information is about.

2.7 Data Assessment

2.7.1 Prior to disclosure, the Town must conduct an assessment that:

a. ensures, to the extent possible, that the identity of any individual who is the subject of the Non-Personal Data cannot be identified or re-identified from the data,

b. identifies the security classification level of the created Non-Personal Data, and

c. identifies the level of risk of re-identification and security measures taken to reduce the risk.

2.7.2 This assessment must be documented on the Creation of Non-Personal Data Tracking Form.

2.8 Data Quality Assurance

2.8.1 When creating Non-Personal Data, the Town will verify and review the effectiveness of any methods used to create the data.

2.8.2 The Town will also ensure methods used to create Non-Personal Data can be replicated for auditing purposes.

2.8.3 The method(s) used to create the data must be documented on the Creation of Non-Personal Data Tracking Form.

3 END OF PROCEDURE AND APPROVAL

Kim Isaak
Chief Administrative Officer

Apr 17, 2026
Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
Apr 17, 2026	Kim Isaak	CAO

CONSENT

POLICY NO	AP-089.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To establish standards for obtaining Consent for the use and/or disclosure of personally identifiable information.

2. POLICY STATEMENT

6.1 The Town of Blackfalds commits to use Personal Information only for the purpose for which the information was collected or compiled or for a Consistent Use.

6.2 The Town understands that in order to use Personal Information for any other purpose (Exceptional Use), or where no other legal authority exists, the individual the information is about must provide their Consent.

6.3 The Town recognizes that processing of Access Requests may require the disclosure of third-party Personal Information.

6.4 In these limited and specific circumstances, the Town must secure the Consent of the Third Party.

3. DEFINITIONS

3.1 "**Access Request**" means a request to access information under the *Access to Information Act*.

3.2 "**Act**" means the *Protection of Privacy Act*.

3.3 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.4 "**Consent**" means the voluntary and informed agreement to engage in an activity or permit an action.

3.5 "**Consistent Use**" means a purpose that has a reasonable and direct connection to the original purpose for which the information was collected.

3.6 "**Director**" means the Employees who are directly responsible for a specific division of the Town.

3.7 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee but does not include an individual who is a member of a class of individuals excluded by regulations.

3.8 "**Exceptional Use**" means limited and specific circumstances in which a public body is permitted to use personal information for a purpose other than the purpose for which it was originally collected, or a consistent use.

3.9 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.10 "**Personal Information**" means recorded information about an identifiable individual, including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.11 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.12 "**Third Party**" means an individual, entity, or organization not directly involved in a primary agreement, transaction, or relationship between two main parties.

3.13 "**Town**" means the municipality of the Town of Blackfalds.

3.14 "**Wet Signature**" means a physical, handwritten signature made with pen and ink (or a similar physical marking tool) on a tangible paper document.

3.15 "**Written Consent**" means consent gathered in written form, often by the signing of a document.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees who are involved in the administration of the *Access to Information Act* and the *Protection of Privacy Act*.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Director and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.3.4 Carry out the duties, powers and responsibilities of the Head of the municipality that are delegated to the position by the Delegation and Assignment of Responsibility, Access to Information Act, and Access to Information Bylaw.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years, or as otherwise required.

5.4.3 In the absence of the Information Governance Coordinator, carry out the duties, powers, and responsibilities of the Head of the municipality that are delegated to the position by the Delegation and Assignment of Responsibility, *Access to Information Act*, and Access to Information Bylaw.

6. POLICY PARTICULARS

6.1 The Town of Blackfalds will develop and implement administrative procedures to guide the process of obtaining Consent for the Exceptional Use and/or disclosure of third-party Personal Information under Sections 12(1)(b) and 13(1)(c) of the *Protection of Privacy Act.*

7. RELATED DOCUMENTS

1.1 *Protection of Privacy Act*
1.2 *Protection of Privacy Regulation AR 132/2025*
1.3 *Protection of Privacy Ministerial Regulation AR 143/2025*
1.4 Consent Procedure
1.5 Statement of Consent
1.6 Statement of Consent for Exceptional Use

8. END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

May 21, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

CONSENT

POLICY NO.	PR-028.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act*, *Protection Privacy Regulation AR 132/*2025 and *Protection of Privacy Ministerial Regulation AR 143/2025*.

1.2 Section 6(2)(a)(iv) of *Protection of Privacy Ministerial Regulation AR 143/2025* stipulates that a privacy management program established by a public body must include policies and procedures related to Consent.

1.3 All referenced definitions can be located in the governing Consent Policy.

2. GENERAL

2.1 Authority-Based Legislation

2.1.1 The *Protection of Privacy Act* is authority-based, meaning the Town may only collect, use or disclose Personal Information if a particular section of the Act authorizes it. Personal Information cannot be collected solely based on Consent.

2.2 Requirements

2.2.1 Consent is only required under the Act in limited circumstances when the Town relies on:

a. Section 12(1)(b) – for the use of Personal Information, or

b. Section 13(1)(c) – for the disclosure of Personal Information.

2.2.2 Consent should be used as a last resort when no other legal authority applies.

2.3 Section 12(1)(b) – Use

2.3.1 Consent will only be accepted in written form.

2.3.2 Where the Town requires Consent to use Personal Information for an Exceptional Use(s), the individual the information is about will be sent a Statement of Consent for Exceptional Use form.

2.3.2 Prior to providing the form, the Information Governance Coordinator (or designate) must outline, specifically, the Personal Information that has been requested for the Exceptional Use(s).

2.3.3 All Exceptional Uses must be listed in the Consent field of the Statement of Consent for Exceptional Use form.

2.3.4 Completed forms must contain a Wet Signature and be returned to the Civic Centre in person.

2.3.5 The Third Party will be asked to provide one (1) piece of government-issued identification to verify their identity.

2.3.6 Only in exceptional cases, forms may be returned via mail, and identity verification can be accomplished through the use of video conferencing technology.

2.3.7 Once the endorsed form has been collected, the Information Governance Coordinator (or designate) must complete the section titled For Office Use Only.

2.3.8 If the third party's identity was validated in any manner other than in person, it must be noted in the Method field.

2.4 Section 13(1)(c) – Disclosure

2.4.1 Consent will only be accepted in written form.

2.4.2 Where the Town requires Consent to disclose third-party Personal Information, the Third Party will be sent a Statement of Consent form.

2.4.3 Prior to providing the form, the Information Governance Coordinator (or designate) must outline, specifically, which records have been requested that contain the individual's Personal Information.

2.4.4 All relevant records must be listed in the Consent field of the Statement of Consent form.

2.4.5 The Information Governance Coordinator (or designate) must also populate the About the Third-Party/Parties Section of the form.

2.4.6 Completed forms must contain a Wet Signature and be returned to the Civic Centre in person.

2.4.7 The Third Party will be asked to provide one (1) piece of government-issued identification to verify their identity.

2.4.8 Only in exceptional cases, forms may be returned via mail, and identity verification can be accomplished through the use of video conferencing technology.

2.4.9 Once the endorsed form has been collected, the Information Governance Coordinator (or designate) must complete the section titled For Office Use Only.

2.4.10 If the third party's identity was validated in any manner other than in person, it must be noted in the Method field.

2.5 Withdrawal and Expiry of Consent

2.5.1 Individuals may withdraw their Consent at any time by contacting the Town in writing.

2.5.2 Consent remains valid unless an individual withdraws their Consent or the expiration date of the Consent, if applicable, has passed.

2.5.3 The Town may choose to set an expiry date for Consent, based on the circumstances and business needs of the Town.

2.6 Retention

2.6.1 If a record of Consent is used to make a decision that directly affects an individual, it must be retained for a period of no less than one (1) calendar year.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak
Chief Administrative Officer

May 21, 2026
Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

CORRECTION OF PERSONAL INFORMATION

POLICY NO	AP-088.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To establish guidelines for the handling of requests to correct an individual's Personal Information.

2. POLICY STATEMENT

2.1 The Town of Blackfalds acknowledges that an individual has the right to request a Correction of Personal Information, not a right to have a Correction made.

2.2 The Town further acknowledges that Corrections can only be made for Factual information, not Opinions pertaining to the individual.

3. DEFINITIONS

3.1 "**Act**" means the *Protection of Privacy Act*.

3.2 "**Annotation**" means the addition of the requested Correction to the original record, close to the information under challenge by the individual.

3.3 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.4 "**Correction**" means the act or result of fixing something that is wrong, inaccurate or mistaken, so that it becomes accurate, acceptable or improved.

3.5 "**Director**" means the Employees who are responsible for a specific division of the Town.

3.6 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee but does not include an individual who is a member of a class of individuals excluded by regulations.

3.7 "**Factual**" means objective, accurate and verifiable using evidence or reliable sources.

3.8 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds.

3.9 "**Link**" means to attach, join or connect a record to the requested Correction.

3.10 "**Opinion**" means a personal belief, judgement, or viewpoint about something.

3.11 "**Personal Information**" means recorded information about an identifiable individual, including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.12 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.13 "**Third Parties**" means individuals, entities, or organizations not directly involved in a primary agreement, transaction, or relationship between two main parties.

3.14 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Directors and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years, or as otherwise required.

5.5 All Employees to:

5.5.1 Understand and adhere to this Policy

6. POLICY PARTICULARS

6.1 The Town of Blackfalds will develop and implement administrative procedures to guide Employees in the handling of requests to correct Personal Information, in accordance with Section 7 of the *Protection of Privacy Act*.

7. RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 Correction of Personal Information Procedure
7.3 Request to Correct Personal Information Form

8. END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

May 21, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

CORRECTION OF PERSONAL INFORMATION

POLICY NO.	PR-027.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act*.

1.2 Section 7 outlines the rights and limitations of an individual to request a Correction of their Personal Information held by the Town.

1.3 Section 7 also outlines the Town's responsibilities when acting on such a request.

1.4 All referenced definitions can be located in the governing Correction of Personal Information Policy.

2. GENERAL

2.1 Factual Information

2.1.1 Requests for Corrections can be made for Factual information, such as age, date of birth, income information or qualifications.

2.1.2 Individuals must provide valid proof in support of Correction requests.

2.1.3 Examples of documents that might be required to substantiate facts include birth certificates or baptismal certificates to prove age or date of birth, or a Notice of Assessment from the Canada Revenue Agency to prove income.

2.1.4 It is not necessary to correct Factual information if the facts are in dispute and it is not possible to otherwise make a Factual determination about the issue or information.

2.2 Opinions

2.2.1 Opinions consist of subjective assessments or evaluations of an individual's condition, abilities, or performance.

2.2.2 The Town cannot correct an Opinion, including an expert or professional Opinion.

2.3 Requests for Correction

2.3.1 Where practical, individuals may ask for Personal Information to be corrected and supply proof through informal means.

2.3.2 Where, in the opinion of the individual, an error or omission exists, a request for Correction should be made to the Town in writing, via the Request to Correct Personal Information form.

2.3.3 Individuals requesting correction of their own Personal Information will be required to provide valid proof of their identity.

2.3.4 Individuals requesting correction of another person's Personal Information must provide proof that they are legally entitled to act on behalf of that person.

2.4 Method of Correction

2.4.1 All records containing Personal Information must be corrected with an Annotation of the date of the Correction.

2.4.2 Annotations should be signed and dated.

2.4.3 Where Personal Information is stored on a medium that is difficult to update, a Link must be used.

2.4.4 Links may consist of a letter or statement from the individual, or a copy of the Request to Correct Personal Information form.

2.5 Notification

2.5.1 The Town must give written notice to the individual within 30 business days of receiving the request that either the Correction has been made or an Annotation or linkage has been made.

2.5.2 Where the Town has previously shared the individual's Personal Information with other municipalities, public bodies or organizations, it is obligated to inform those parties of the individual's request for Correction or Annotation.

2.5.3 Third Parties should be notified within 30 business days.

2.5.4 Third-party notification is not required if the Correction, Annotation or Link is not material or if the individual agrees, in writing, that notification is unnecessary.

2.5.5 Once notified, Third Parties must make any Correction, Annotation or Link to the Personal Information in their custody or under their control.

2.6 Refusal

2.6.1 The Town may refuse Correction requests that do not pertain to Personal Information, have not been substantiated with adequate proof, or consist of Opinion rather than fact(s).

2.6.2 When the Town is dissatisfied with the proof presented, Town staff will not change the information but use an Annotation or Link to connect the presented information with the original information.

2.6.3 In terms of Opinion, the Town may describe the information in dispute and place the description, along with a statement that the individual does not agree with the Opinion or interpretation, on the record.

2.6.4 The Town is required to note only the part of the requested Correction that is relevant to the record being annotated or the Link being made.

2.7 Role of the Information and Privacy Commissioner

2.7.1 The Information and Privacy Commissioner has the power to review the Town's actions with respect to requests for Correction of Personal Information, including the decision to refuse Correction.

2.7.2 The Commissioner's Office also retains the power to extend the timeline for responding to requests for Correction of Personal Information.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak
Chief Administrative Officer

May 21, 2026
Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

PRIVACY IMPACT ASSESSMENT

POLICY NO	AP-090.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. POLICY PURPOSE

1.1 To establish guidelines for the implementation and use of Privacy Impact Assessments.

2. POLICY STATEMENT

2.1 The Town of Blackfalds recognizes and acknowledges that to remain compliant with legislated requirements, Privacy Impact Assessments must be implemented in accordance with Section 26 of the *Protection of Privacy Act*.

3. DEFINITIONS

3.1 "**Act**" means the *Protection of Privacy Act*.

3.2 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.3 "**Commissioner**" means Alberta's **I**nformation and Privacy Commissioner.

3.4 "**Common or Integrated Program or Service**" means a program or service that is planned, administered, delivered, managed, monitored, or evaluated collaboratively by one public body together with one or more other public body.

3.5 "**Data Matching**" means linking Personal Information between two or more databases or other electronic sources of information.

3.6 "**Director**" means the Employees who are responsible for a specific division of the Town.

3.7 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee but does not include an individual who is a member of a class of individuals excluded by regulations.

3.8 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.9 "**OIPC**" means the Office of the Information and Privacy Commissioner.

3.10 "**Personal Information**" means recorded information about an identifiable individual including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.11 "**Privacy Impact Assessment**" means a systematic process used to identify, evaluate, and mitigate privacy risks associated with the collection, use, disclosure, retention and disposition of Personal Information captured in a program, system, project, or process.

3.12 "**Regulations**", for the purposes of this Policy, means *Protection of Privacy Ministerial Regulation AR 143/2025*.

3.13 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.14 "**Significant Harm**", according to the Act, includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to, or loss of property or other legal harms or financial losses.

3.15 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Director and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years, or as otherwise required.

5.5 All Employees to:

5.5.1 Understand and adhere to this Policy.

6. POLICY PARTICULARS

6.1 The Town of Blackfalds will develop and implement administrative procedures to guide the implementation and compliant use of Privacy Impact Assessments.

7. RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 *Protection of Privacy Ministerial Regulation AR 143/2025*
7.3 Privacy Impact Assessment Procedure
7.4 Privacy Impact Assessment Questionnaire
7.5 Personal Information Flow
7.6 Security Risk Grid
7.7 OIPC Privacy Impact Assessment Template

8. END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

May 21, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

PRIVACY IMPACT ASSESSMENT

POLICY NO.	PR-029.26
DIVISION DEPARTMENT	Administration/Information Technology
REVIEW PERIOD	Every 3 Years/Upon Legislative Change/As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act* and *Protection of Privacy Ministerial Regulation AR 143/2025*.

1.2 Section 26(1) of the Act stipulates that a public body must prepare a Privacy Impact Assessment in prescribed circumstances and, if required by the Regulations, submit it to the Commissioner.

1.3 The Town must provide the Commissioner with a copy of the requested Privacy Impact Assessment within 30 business days of a request made under Section 27(1)(j) of the Act.

1.4 Section 7(2) of the Regulations outlines the requirements public bodies must meet when developing Privacy Impact Assessments.

1.5 All referenced definitions can be located in the governing Privacy Impact Assessment Policy.

2. GENERAL

2.1 Compliance

2.1.1 The Town must prepare a Privacy Impact Assessment (PIA) 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 if one or more of the following apply:

a. the loss of, unauthorized access to or unauthorized disclosure of the Personal Information could result in Significant Harm as determined in accordance with Section 4 of the Regulations;

b. one or more of the factors requiring submission of a Privacy Impact Assessment to the Commissioner established by Section 7(5) of the Regulations apply.

2.2 Requirements

2.2.1 A Privacy Impact Assessment must:

a. be completed prior to the implementation of, or substantial change to, an administrative practice, project, program or service,

b. include a summary of the purpose of the collection, use or disclosure of Personal Information,

c. identify the types of Personal Information that will be collected, used or disclosed and reasonable security arrangements in place to protect that information,

d. identify the legal authority for the collection, use or disclosure of the Personal Information,

e. identify any privacy risks and mitigation strategies respecting the Personal Information,

f. identify administrative, physical or technical safeguards in place to protect the Personal Information, including how it will be securely transmitted, matched or linked by the Town, if applicable,

g. describe accuracy, correction and retention procedures that will be implemented to ensure the Personal Information is accurate and complete, and

h. establish a clear governance structure respecting the responsibilities and accountability of the Town if engaging in a Common or Integrated Program or Service or if the Town is collecting Personal Information from another public body for the purpose of Data Matching.

2.3 Submission to the Commissioner

2.3.1 The Town must submit a Privacy Impact Assessment to the Commissioner's Office if one or more of the following factors apply:

a. an administrative practice, program or service will collect, use or disclose Personal Information deemed to be of high sensitivity;

b. an administrative practice, program or service will involve the Personal Information of a significant percentage of the Town's population;

c. an administrative practice, program or service is part of a Common or Integrated Program or Service;

d. an administrative practice, program, project or service involves the development or use of innovative technology;

e. the Commissioner requests a copy of a Privacy Impact Assessment under Section 27(1)(j) of the Act.

2.3.2 Privacy Impact Assessments submitted to the Commissioner must use the OIPC Privacy Impact Assessment Template or they will not be accepted.

2.4 Completion

2.4.1 Responsibility for completing Privacy Impact Assessments should be assigned to employees who possess a strong knowledge or familiarity with the particular administrative practice, project, program or service.

2.4.2 All fields must be filled in as prescribed, with no omissions.

2.4.3 Attachments or appendices that accompany PIA questionnaires must also be completed, as prescribed.

2.4.4 Where applicable, employees and Department Heads should sign and date completed PIA submissions.

2.4.5 Incomplete submissions will not be endorsed by the Information Governance Coordinator or accepted by the Commissioner's Office and will be returned to department staff for completion.

2.5 Revisions

2.5.5 Where the Information Governance Coordinator or Privacy Commissioner identify risks to the security of Personal Information that have not been accounted for, responsible departments will receive notice in writing.

2.5.6 Submissions must be amended to clearly demonstrate that security concerns have been adequately considered and addressed.

2.6 Approvals

2.6.1 Implementation of new, or substantial change(s) to, administrative practices, projects, programs or services must not proceed until they receive written authorization.

2.6.2 The Information Governance Coordinator, in consultation with the CAO, will authorize the Town's PIA Questionnaires.

2.6.3 The Privacy Commissioner will provide authorization for OIPC PIA Templates.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak

Chief Administrative Officer

May 21, 2026

Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
May 21, 2026	Kim Isaak	CAO

PRIVACY INCIDENT

POLICY NO	AP-091.26
DIVISION DEPARTMENT	Administration/Records Management
REVIEW PERIOD	Every 3 Years, upon legislative change or as required.

1. POLICY PURPOSE

1.1 To establish guidelines for Privacy Incident response and notification.

2. POLICY STATEMENT

2.1 The Town of Blackfalds recognizes that Privacy Incidents may result in harm(s) to the municipality that include operational disruption, financial loss, legal consequences and reputational damage.

2.2 The Town also acknowledges that Privacy Incidents may result in harm(s) to individuals such as identity theft, loss of employment, financial loss, emotional or psychological harm, loss of privacy and reputational damage.

3. DEFINITIONS

3.1 "**Act**" means the *Protection of Privacy Act*.

3.2 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.3 "**Commissioner**" means Alberta's Information and Privacy Commissioner.

3.4 "**Data Derived from Personal Information**" means data created by Data Matching which identifies any individual whose Personal Information was used in the Data Matching.

3.5 "**Data Matching**" means linking Personal Information between two or more databases or other electronic sources of information.

3.6 "**Director**" means the Employees who are responsible for a specific division of the Town.

3.7 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee but does not include an individual who is a member of a class of individuals excluded by regulations.

3.8 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.9 "**Manager**" means the Employees who are directly responsible for managing a specific department of the Town.

3.10 "**Minister**", for the purposes of this Policy, means the Minister of Technology and Innovation.

3.11 "**OIPC**" means the Office of the Information and Privacy Commissioner.

3.12 "**Personal Information**" means recorded information about an identifiable individual including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.13 "**Privacy Incident**", otherwise referred to as a breach, means loss of, unauthorized access to, or unauthorized disclosure of Personal Information.

3.14 "**Real Risk of Significant Harm**" means a legal threshold used to decide whether a Privacy Incident must be reported to regulators and impacted individuals.

3.15 "**Regulations**", for the purposes of this Policy, means Protection of Privacy Ministerial Regulation AR 143/2025.

3.16 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.17 "**Significant Harm**", according to the Act, includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to, or loss of property or other legal harms or financial losses.

3.18 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Director and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure implementation of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every three years, or as otherwise required.

5.5 All Employees to:

5.5.1 Understand and adhere to this Policy.

6. POLICY PARTICULARS

6.1 The Town of Blackfalds will develop and implement Administrative Procedures to guide legislated Privacy Incident response and notification.

7. RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 *Protection of Privacy Ministerial Regulation AR 143/2025*
7.3 Privacy Incident Procedure

8. END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

Jun 10, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
Jun 10, 2026	Kim Isaak	CAO

PRIVACY INCIDENT

POLICY NO.	PR-030.26
DIVISION DEPARTMENT	Administration/Records Management
REVIEW PERIOD	Every 3 Years, upon legislative change or as required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act* and *Protection of Privacy Ministerial Regulation AR 143/2025*.

1.2 According to Section 10(2) of the Act, a privacy incident occurs when Personal Information, or Data Derived from Personal Information, under the custody or control of a public body is lost, accessed or disclosed without authorization.

1.3 In accordance with Sections 4(3) of the Regulations, notification of privacy incidents must be provided to affected parties.

1.4 Where Real Risk of Significant Harm to an individual exists (RROSH), notification must also be sent to the Commissioner and the Minister in accordance with Sections 4(4) and 4(5) of the Regulations.

1.5 All referenced definitions can be located in the governing Privacy Incident Administrative Policy.

2. GENERAL

2.1 Incident Response

2.1.1 Appropriate response to Privacy Incidents consists of six key steps.

a. Containment
b. Initial Reporting
c. Investigation and Evaluation of Risk
d. Notification
e. Additional Measures
f. Prevention

2.2 Containment

2.2.1 As soon as a Privacy Incident is identified, limiting the extent and impact of the breach is a priority.

2.2.2 Employees who become aware of a Privacy Incident should notify their Manager or Director immediately.

2.2.3 Employees will take necessary actions to immediately contain and document the details of the incident.

2.2.4 Other program areas that may need to be involved in containment of the incident must be identified and contacted.

2.3 Initial Reporting

2.3.1 Prompt reporting of a Privacy Incident is essential to ensure timely containment.

2.3.2 Notified Managers and/or Directors will report the incident to the Information Governance Coordinator, providing all necessary and relevant details.

2.3.3 If there is uncertainty determining whether a situation meets the criteria for a Privacy Incident, Managers and/or Directors should consult the Information Governance Coordinator who will assist with the determination.

2.3.4 Information Technology must be contacted immediately if the incident involves an IT system, device, or application that may have been compromised.

2.3.5 If the Privacy Incident involves suspected criminal activity of any kind, the RCMP must also be contacted and notified.

2.4 Investigation and Evaluation of Risk

2.4.1 The Information Governance Coordinator will:

a. gather all relevant information to determine the nature and extent of the incident,

b. prepare an analysis of harm and evaluate whether the incident meets the threshold for Real Risk of Significant Harm (RROSH),

c. notify the CAO of the incident, it's scope and associated harm(s),

d. consult legal counsel, where practical, and

e. provide recommendations to Managers, Directors and Employees, including but not limited to, additional mitigation measures and steps to prevent reoccurrence.

2.5 Notification – Real Risk of Significant Harm (RROSH)

2.5.1 If, based on the analysis of harm, a Privacy Incident meets the threshold for Real Risk of Significant Harm, the Town must notify the impacted individual(s), the Commissioner, and the Minister.

2.5.2 Notifications must comply with the requirements of Sections 4(3), 4(4) and 4(5) of the Regulations, respectively.

2.5.3 Notifications to impacted individuals and the Commissioner will be issued by the Information Governance Coordinator.

2.5.4 Notifications to the Minister will be issued by the CAO, as head of the public body.

2.6 Notification – No Real Risk of Significant Harm

2.6.1 In cases where a Privacy Incident does not meet the threshold for Real Risk of Significant Harm, the Town may choose to notify impacted individuals to promote transparency, accountability, and further minimize the harm(s) an incident may cause.

2.6.2 The Town may also choose to voluntarily notify the Commissioner.

2.6.3 Voluntary notification(s) must meet the requirements of Sections 4(3) and 4(4) of the Regulations, respectively and will be issued by the Information Governance Coordinator.

2.7 Additional Measures

2.7.1 Depending on the severity of the Privacy Incident, the Information Governance Coordinator or legal counsel may recommend additional mitigation measures, such as credit monitoring where an individual's Social Insurance Number or financial information has been compromised.

2.7.2 While circumstances may vary, appropriate mitigation measures may also vary. As such, consideration will occur on a case-by-case basis.

2.8 Prevention

2.8.1 Following the completion of investigations, the Town will develop and implement preventative measures to minimize the risk of reoccurrence.

2.8.2 Preventative measures may include, but are not limited to, updating policies or procedures, improving safeguards, and/or additional training for Employees.

2.9 Retention

2.9.1 Records pertaining to Privacy Incidents will be retained for a period of 5 calendar years, in accordance with the Town's Functional File Plan.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak
Chief Administrative Officer

Jun 3, 2026
Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
Jun 3, 2026	Kim Isaak	CAO

AUTOMATED SYSTEMS AND SAFEGUARDS

POLICY NO	AP-094.26
DIVISION DEPARTMENT	Administration/Records Management
REVIEW PERIOD	Every 4 Years, Upon Legislative Change or As Required

1. POLICY PURPOSE

1.1 To establish guidelines for the identification of Automated Systems that collect Personal Information, along with their associated safeguards, and for determining how Automated Systems may use Personal Information to generate content and/or enable Town Employees to make decisions, recommendations, or predictions based on that information.

2. POLICY STATEMENT

2.1 The Town of Blackfalds recognizes that it employs numerous Automated Systems in its Computing Environment, which collect Personal Information.

2.2 The Town acknowledges that adequate technical safeguards must be in place to protect the Personal Information housed in Automated Systems.

2.3 The Town also understands that governance is required in instances where Automated Systems will use Personal Information to generate content or where Town Employees will rely on information housed in Automated Systems to make decisions, recommendations or predictions.

3. DEFINITIONS

3.1 "**Act**" means the *Protection of Privacy Act*.

3.2 "**Automated System**" means a system that performs tasks or processes automatically with little or no human intervention, using a combination of machines, software, sensors, and control mechanisms to operate efficiently and consistently.

3.3 "**CAO**" means the Chief Administrative Officer of the Town of Blackfalds, appointed by Council as per the *Municipal Government Act*.

3.4 "**Computing Environment**" means the overall setup in which a program or system runs, including its hardware, software, and configuration.

3.5 "**Director**" means the Employees who are responsible for a specific division of the Town.

3.6 "**Employee**" as defined in Section d.1(k) of the Alberta Employment Standards Code, means an individual employed to do work who receives or is entitled to wages and includes a former employee, but does not include an individual who is a member of a class of individuals excluded by regulations.

3.7 "**Information Governance Coordinator**" means the individual designated, in writing, to administer the provisions of the *Access to Information Act* and the *Protection of Privacy Act* on behalf of the Town of Blackfalds.

3.8 "**Manager**" means the Employees who are directly responsible for managing a specific department of the Town.

3.9 "**Personal Information**" means recorded information about an identifiable individual including, but not limited to, the individual's name, home or business address, home or business telephone number, home or business email address, race, national or ethnic origin, age, sex, gender identity, marital status, biometric information and medical, educational, financial or criminal history.

3.10 "**Privacy Management Program**" means a framework of policies and procedures that clearly demonstrate the Town's compliance with the provisions of the *Protection of Privacy Act*.

3.11 "**Regulations**", for the purposes of this Policy, means *Protection of Privacy Ministerial Regulation AR 143/2025*.

3.12 "**Senior Legislative Advisor**" means the individual designated, in writing, to administer the provisions of the Access to Information Act and the Protection of Privacy Act on behalf of the Town of Blackfalds in the absence of the Information Governance Coordinator.

3.13 "**Town**" means the municipality of the Town of Blackfalds.

4. SCOPE

4.1 This Policy applies to all Town of Blackfalds Employees.

5. AUTHORITY AND RESPONSIBILITIES

5.1 Chief Administrative Officer to:

5.1.1 Approve this Policy.

5.1.2 Ensure Policy review occurs and verify the implementation of this Policy.

5.2 Directors and Managers to:

5.2.1 Understand and adhere to this Policy.

5.2.2 Ensure implementation of this Policy.

5.3 Information Governance Coordinator to:

5.3.1 Understand and adhere to this Policy.

5.3.2 Ensure employees are aware of this Policy.

5.3.3 Make recommendations to the CAO of necessary Policy amendments.

5.4 Senior Legislative Advisor to:

5.4.1 Understand and adhere to this Policy.

5.4.2 Ensure this Policy is reviewed every four years, or as otherwise required.

5.5 All Employees to:

5.5.1 Understand and adhere to this Policy.

6. POLICY PARTICULARS

6.1 The Town of Blackfalds will develop and implement Administrative Procedures to identify Automated Systems that collect Personal Information and their related technical safeguards.

6.2 The Administrative Procedures will also identify Automated Systems that use Personal Information to generate content and those that enable Town Employees to make decisions, recommendations, or predictions based on the information housed within.

7. RELATED DOCUMENTS

7.1 *Protection of Privacy Act*
7.2 *Protection of Privacy Ministerial Regulation AR 143/2025*
7.3 Automated Systems and Safeguards Procedure

8. END OF POLICY AND APPROVAL

Kim Isaak
Chief Administrative Officer

June 11, 2026
Date

POLICY RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
June 11, 2026	Kim Isaak	CAO

AUTOMATED SYSTEMS AND SAFEGUARDS

PROCEDURE NO.	PR-033.26
DIVISION DEPARTMENT	Administration/Access and Records Management
REVIEW PERIOD	Every 4 Years, Upon Legislative Change or As Required

1. PREAMBLE

1.1 The Town of Blackfalds is subject to the provisions of the *Protection of Privacy Act* and *Protection of Privacy Ministerial Regulation AR 143/2025*.

1.2 Section 10(1) of the *Protection of Privacy Act* states that a public body must protect Personal Information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

1.3 Section 6(1)(b)(iii) of the Regulations stipulates that a Privacy Management Program established by a public body under Section 25 of the Act must include policies and procedures for how Automated Systems will use Personal Information, including any security or technical safeguards that will be implemented to protect Personal Information, if the Town will use the information in an Automated System to generate content or make decisions, recommendations or predictions.

1.4 All referenced definitions can be located in the governing Automated Systems and Safeguards Policy.

1.5 The Automated Systems and Safeguards Matrix is attached to, and forms part of, this Procedure as Schedule "A". Schedule "A" establishes the prescribed Automated Systems, safeguards and control measures associated with the application of this Procedure.

2. GENERAL

2.1 Computing Environment

2.1.1 The Town's current Computing Environment houses 16 Automated Systems that collect and/or use Personal Information.

2.2 Generated Content

2.2.1 Catalis and Central Square (Diamond) utilize Personal Information to generate utility billing statements, tax notices and arrears letters.

2.2.2 First Due uses Personal Information to generate provincial fire reports, patient medical care reports, and billing reports. Where desired, the platform allows for redaction(s) of Personal Information, including that of responding fire personnel.

2.2.3 Genetec/I-Pro utilizes Personal Information to produce video footage generated by systems installed in Municipal Enforcement vehicles and officers' body-worn cameras.

2.2.4 HRISMyWay uses Personal Information to generate paystubs and T4 Statements for all Town Employees.

2.2.5 Microsoft Exchange manages the entire Microsoft suite of products. Personal Information may be collected through Outlook email correspondence and used to generate responses, where appropriate.

2.2.6 Omnigo uses Personal Information to generate documentation used for court appearances/trials.

2.2.7 Sensus Analytics synchronizes with Catalis and Central Square (Diamond) to enable generation of utility billing based on residential/commercial water usage.

2.2.8 GeoVision GV-NVR generates video surveillance footage for investigative and evidentiary purposes.

2.3 Decisions, Recommendations and Predictions

2.3.1 In specific instances, Personal Information generated by Genetec/I-Pro may be used to make decisions regarding citations, fines or related consequences.

2.3.2 Scout Talent utilizes Personal Information to assist with Human Resources recruiting, including reference checks.

2.3.3 Trakstar Perform contains Personal Information for all Town Employees and is used for appraisal of job performance. Recommendations may consist of areas for improvement or incremental salary increases.

2.3.4 GeoVision GV-NVR contains Personal Information, in the form of video captures and footage, that may be used to make decisions regarding citations, fines or related consequences. Additional decisions may result in provision of footage to the Royal Canadian Mounted Police (RCMP) for pursuit of civil and/or criminal action.

2.4 Policy Updates

2.4.1 When Automated Systems that collect and/or use Personal Information are added to, or removed from, the Town's Computing Environment, Directors must inform the Information Governance Coordinator.

2.4.2 The Information Governance Coordinator will ensure that the Automated Systems and Safeguards Matrix (Schedule "A") is maintained and that updates are forwarded for CAO approval, as required.

3. END OF PROCEDURE AND APPROVAL

Kim Isaak

Chief Administrative Officer

June 11, 2026

Date

PROCEDURE RECORD HISTORY

Date Approved/Revised:	Approved/Reviewed By:	Title:
June 11, 2026	Kim Isaak	CAO

BLACKFALDS
ALBERTA

AUTOMATED SYSTEMS AND SAFEGUARDS MATRIX

Platform	Use	External Certification(s)	Environmental Security
ASWeb	Security Fob Building Access	No external certifications. Meets internal IT security standards.	Hosted in secured network environment with firewall protection, access controls, and controlled physical access.
Catalis	Financial functions excluding payroll	AICPA SOC Type 1, AICPA SOC Type 2	Cloud-based platform hosted in secure facilities with restricted access, encryption, multi-factor authentication, monitoring, vulnerability scanning, penetration testing, (Amazon Web Services) AWS-native security tools, backups.
Central Square (Diamond)	Financial functions including payroll and point-of-sale transactions	No external certifications. Meets internal IT security standards.	Hosted (on premises) within the Town's computing environment, with secure access managed by IT and designated Diamond Administrators. Security measures include access controls, network controls, and system monitoring.
Corepoint	Safety/Certification Tracking	*< None publicly available>*	Vendor-hosted, secure environment with role-based access control, monitoring, intrusion detection, encryption, firewalls, network isolation, and environment separation.
First Due	Fire Investigation, Tracking and Reporting	SOC 2 Type II	Cloud-based platform hosted in secure facilities with controlled physical access, redundancy, and disaster recovery.
Genetec/I-Pro	In-Car and Bodycam Video Footage	ISO/IEC 27001, ISO/IEC 27017, SOC 2 Type II, UL 2900	Vendor-hosted, secure cloud environment with role-based access, encryption of video data at rest and in transit, audit logging, and monitoring to ensure integrity and availability of evidence.
HRISMyWay	Employee Time Tracking	Vendor Security Compliance Attestation, SOC 2 Where Applicable	Vendor-hosted, secure environment with restricted access, monitoring, encryption, and documented incident response. HRISMyWay synchronizes data with Diamond through secured system integrations.
Microsoft Exchange	Complete Microsoft suite, including Outlook	ISO 27001, SOC 1, SOC 2, SOC 3, ISO 27701	Microsoft-managed, global data centres with biometric access, 24/7 monitoring, encryption at rest and in transit, redundancy, and regular security audits.
Omnigo	Municipal Enforcement	Vendor Security Compliance Attestation	Secure, vendor-hosted infrastructure with access controls, monitoring, and backup processes.
Perfect Mind	Abbey Centre Memberships	SOC 2 Type II Where Applicable	Secure, cloud-hosted environment with encrypted data storage, controlled physical access, and business continuity processes.
PSD Citywide	Maintenance Issue Reporting and Tracking	No external certifications. Meets internal IT security standards.	Cloud-based platform hosted in a vendor-managed environment with vendor-provided security controls and support, including controlled access, system monitoring, backups, and incident response.

BLACKFALDS ALBERTA

AUTOMATED SYSTEMS AND SAFEGUARDS MATRIX

Platform	Use	External Certification(s)	Environmental Security
Scout Talent	Human Resources Recruiting	ISO 27001, SOC 2 Type II	Cloud-based platform hosted in vendor-managed data centres with physical controls, redundancy, environmental safeguards, and disaster recovery.
Sensus Analytics	Water Meter Synchronization	Vendor Security Compliance Attestation	Cloud-based, secure infrastructure with encryption, monitoring, and access restrictions. Sensus synchronizes data with Catalis and Diamond through secured system integrations.
Trakstar Perform	Employee Performance Review	SOC 2 Type II	Cloud-based platform hosted in vendor-managed infrastructure with encrypted data storage, role-based access, monitoring, and backup controls.
Versatile ERMS	Electronic Records and Information Management	AICPA SOC 2 Type 2, Silent Sector Penetration Test Verification	Vendor-managed, secure data centres with encryption, 24/7 monitoring, restricted physical access, redundancy, and disaster recovery.
GeoVision GV-NVR	CCTV Video Surveillance Recording and Management	Vendor Security Compliance Attestation, Where Applicable	On-premise video management system with controlled access, monitoring and secure storage of surveillance footage. Supports audit-logging, role-based permissions, and system hardening to ensure integrity and availability of recorded video for operational and Investigative purposes.