ONTARIO · MFIPPA S.28(3)

Privacy Impact Assessment

A pre-filled working template for an Ontario municipal institution assessing the TrueNorth Civic AI platform. Vendor facts are completed; institution-specific fields are marked for your review.

Institution	[Insert municipality name]
Service assessed	TrueNorth Civic AI
Assessment date	[Insert date]
Status	Draft for review — not legal advice

Contents

How to use this template 3

1. Institution and service information 3

2. Scope and method 3

3. Element 1 — Purpose and necessity 4

4. Element 2 — Legal authority 5

5. Element 3 — Personal information inventory 5

6. Element 4 — Sources of personal information 6

7. Element 5 — Access and position titles 6

8. Element 6 — Limitations and restrictions 6

9. Element 7 — Retention period 7

10. Element 8 — Safeguards and risks to individuals 8

11. Element 9 — Prevention and mitigation 11

12. Element 10 — Other prescribed information 11

13. Residual jurisdictional risk and decision 12

14. Sign-off 12

Appendix A: Documents reviewed 12

How to use this template

This PIA is prepared for Ontario municipal institutions considering or deploying TrueNorth Civic AI. Vendor facts (architecture, safeguards, retention) are completed; institution-specific fields are marked [Insert ...] for completion by the municipality's privacy lead and head of institution. Complete every bracketed field, delete categories that are not in scope, record the approval decision, and retain the signed assessment with the procurement file. Update it before any significant change to the purpose for which personal information is used or disclosed, and provide a copy to the Information and Privacy Commissioner of Ontario on request. This template supports, but does not replace, the municipality's own PIA process. It is not legal advice.

1. Institution and service information

Institution	[Insert legal name of municipality]
Head of institution / delegate	[Insert name and title]
Assessment completed by	[Insert name, title, department]
Privacy review	[Insert name and title]
IT / security review	[Insert name and title, or "not applicable — no IT function"]
Service under assessment	TrueNorth Civic AI — a cloud AI workspace for municipal staff providing cited research, document drafting, meeting transcription/ minutes and workflow automation.
Programs in scope	[Insert departments, programs or functions]
Users in scope	[Insert number of users and roles]
Vendor privacy contact	support@truenorthcivicai.ca
Assessment date	[Insert date] Version: [Insert] Next review: [Insert]

2. Scope and method

This assessment covers the TrueNorth Civic AI platform as configured for the institution, including the web application, the AI processing pipeline, document storage and the vendor's support arrangement. It does not assess other municipal systems that may exchange records with the platform. The assessment follows the ten content elements prescribed by MFIPPA s.28(3). Written PIAs become expressly mandatory for Ontario municipal institutions on January 1, 2027, and must be updated before a significant change in purpose. A content map is provided as a table in this document.

TABLE 1 · MFIPPA S.28(3) CONTENT MAP

Element	MFIPPA s.28(3) requirement	Where addressed
1	Purpose for collecting, using or disclosing personal information and why it is necessary	Section 3
2	Legal authority relied on	Section 4
3	Types of personal information and how each type is used or disclosed	Section 5
4	Sources of the personal information	Section 6
5	Position titles of officers, employees, consultants or agents with access	Section 7
6	Limitations or restrictions on collection, use or disclosure	Section 8
7	Period of retention	Section 9
8	Administrative, technical and physical safeguards, and risks to individuals	Section 10
9	Steps to prevent or reduce theft, loss or unauthorized use/ disclosure and mitigate risks	Section 11
10	Any other prescribed information	Section 12

3. Element 1 — Purpose and necessity

Purpose of the collection and use	[Insert a plain-language statement. Example: The municipality uses TrueNorth to support staff research, drafting, meeting minutes and routine correspondence. The platform processes staff account information and the content staff choose to submit. Personal information may be included where it is necessary for the municipal purpose being served.]
Why the information is necessary	[Explain why the records cannot reasonably be de-identified or handled without the platform. Example: the records are inherently about identifiable individuals — correspondence, service requests, bylaw files, meeting minutes — and removing all identifiers would make them unusable for the municipal purpose.]
Out of scope	automated decision-making about individuals without human review; health information unless specifically assessed; law enforcement sensitive records unless specifically assessed; any purpose unrelated to the programs listed in Section 1.

4. Element 2 — Legal authority

MFIPPA permits collection where it is expressly authorized by statute, for law enforcement, or necessary to the proper administration of a lawfully authorized activity (s.28).

Enabling statute or bylaw	[Insert — e.g., Municipal Act, 2001, S.O. 2001, c. 25, s. ...; or a specific bylaw]
Program authority	[Insert council resolution, bylaw or delegated authority]
Collection authority for staff account data	[Insert, typically the municipality's employment/administration authority]
Use authority	[Insert — consistent with the purpose for which the information was collected (MFIPPA s.31)]
Disclosure authority, if any	[Insert, or state "no disclosure beyond the service provider arrangement"]
Vendor relationship	TrueNorth acts as a service provider processing information on the institution's behalf. Record the contractual basis and confirm that disclosure to the vendor is limited to what is necessary for the service.

5. Element 3 — Personal information inventory

1. Staff account data — name, work email, department, job title, optional profile photo. Used for account administration and display.
2. User-generated content — chat questions, drafts, uploaded records, meeting transcripts. May contain third-party personal information (resident names, addresses, phone numbers, correspondence) when staff process municipal records. Used to perform the requested research, drafting or analysis.
3. Support and feedback data — support correspondence and feedback submissions. Used to resolve issues and improve the service.
4. Audit and telemetry data — timestamps, user identifiers and action logs. Used for governance reporting, incident investigation and access requests.
5. Special categories — [Identify any health, law enforcement or other sensitive records in scope, or state "none"].

6. Element 4 — Sources of personal information

Directly from the individual	residents, applicants, complainants and contractors who provide information in the course of a service request, application, correspondence or hearing.
Municipal records	existing files that staff upload or reference — council reports, correspondence, bylaw files, service records.
Staff members	account information provided by employees and council staff.
Public sources	[Insert any public registries, provincial databases or published materials, or state "none"].
Indirect collection	[If information is collected indirectly, identify the source and the authority. Otherwise state "none"].

7. Element 5 — Access and position titles

[Insert each position title, its platform role and the basis for access.] Example rows: Clerk / Deputy Clerk — Admin — tenant administration, user management, audit review. CAO / Department Head — Staff or Admin — program oversight and document review. Administrative Assistant — Staff — day-to-day drafting, research and correspondence. TrueNorth support personnel — vendor support (restricted) — support and incident investigation only, under confidentiality obligations and audit logging. Where one person holds both Admin and Staff roles, record that arrangement and confirm that audit records still distinguish administrative actions from ordinary use.

8. Element 6 — Limitations and restrictions

Purpose limitation	use is limited to the programs listed in Section 1. A new use requires an update to this PIA before it begins.
User limitation	access is limited to named staff accounts. Accounts are removed when a user leaves the role; SSO, where used, follows the municipality's directory.
Content limitation	[State any records that must not be uploaded — e.g., health records, law enforcement files, material subject to a legal hold.]
Disclosure limitation	no disclosure to other customers, no sale of data, no use for model training, no advertising use.
Geographic limitation	production storage and processing are pinned to Canada (northamerica-northeast1, Montréal).
Retention limitation	as set out in Section 9.

9. Element 7 — Retention period

Chat threads	30 days, then automatic purge.
Uploaded documents and generated drafts	90 days by default, configurable by agreement.
Meeting transcripts	per tenant configuration; deletable by tenant administrators.
Audit logs	retained per the institution's governance requirements.
Contract termination	vendor deletes tenant content and confirms disposal in writing.
Institution decision	[Confirm these defaults against the municipality's records schedule. Where a record class must be retained longer, export it to the municipality's records management system rather than relying on the platform as the system of record.]

TABLE 2 · RETENTION SCHEDULE

Record type	Platform default	Institution decision
Chat threads	30 days, then automatic purge	[Confirm or adjust by agreement]
Uploaded documents and generated drafts	90 days, configurable	[Confirm against records schedule]
Meeting transcripts	Per tenant configuration	[Insert]
Audit logs	Per governance requirement	[Insert]
Content at termination	Deleted, written confirmation	[Confirm disposal sign-off]

10. Element 8 — Safeguards and risks to individuals

Technical safeguards	TLS 1.3 in transit; AES-256 at rest; CMEK on qualifying plans; Cloud DLP redaction before model calls; role-based access (Staff/Admin/ Super Admin); per-request tenant isolation; audit logging; Google Secret Manager; private-range VPC egress.
Residency	production pinned to GCP northamerica-northeast1 (Montréal); environment validation refuses non-Canadian production regions.
Model handling	zero-training guarantee; web grounding disabled by default on sensitive workflows.
Administrative safeguards	named accounts; documented role assignment; staff orientation; vendor confidentiality and data-processing terms; breach-response procedure aligned to the RROSH threshold.
Physical safeguards	Google Cloud data centres in the Montréal region provide physical access, environmental and media-disposal controls. Office devices used to access the platform remain subject to the municipality's device and premises policies.
Risks to individuals	see the Risk Register table in this document. Record the institution's rating and decision for each risk.

TABLE 3 · PERSONAL INFORMATION FLOW MAP

Stage	System / Service	Location	Safeguards
Sign-up & identity	Firebase Authentication (work email, verified) with optional Microsoft Entra ID (Azure AD) SSO	Canada / global identity service	Government-organization email verification; optional Microsoft 365 work-account sign-in matched to the tenant by verified email domain; minimal profile data (name, work email, department, job title)
Transmission	HTTPS to the TrueNorth API and Firebase	In transit to GCP northamerica-northeast1	TLS 1.3 encrypted transport; HSTS
Pre-processing	Cloud DLP inspection & redaction before any model call	Google Cloud DLP global endpoint (processing not region-pinned); results stored in Montréal	Canadian identifiers (SIN, provincial health number, addresses, contact info) detected and redacted prior to AI processing
AI processing	Vertex AI (Gemini models) with web grounding disabled by default on sensitive workflows	US/EU multi-regions (Gemini 3.x via the Vertex AI global endpoint; embeddings run in Montréal)	Zero model training on customer data; prompts and outputs are Customer Data and not retained by the model provider beyond transient processing; DLP pre-redaction runs before every model call
Document storage	Cloud Storage + PostgreSQL (documents, RAG indexes)	northamerica-northeast1 (Montréal)	AES-256 at rest; customer-managed encryption keys (CMEK) on qualifying plans; tenant isolation
Retention & purge	Scheduled data-retention jobs	northamerica-northeast1 (Montréal)	Chat threads auto-purged after 30 days; uploaded documents retained 90 days (configurable by agreement); deletion on request or at termination

TABLE 4 · RISK REGISTER

Risk	Potential harm	Mitigation	Residual rating / decision
Unauthorized access to tenant content	Exposure of personal or sensitive municipal information	Named accounts; role-based access; tenant isolation per request; audit logging; account removal on role change	[Insert rating and accept/mitigate/ reject]
Accidental disclosure through staff error	Resident information sent to the wrong recipient or context	Staff orientation; DLP pre-processing; review before sending or publishing; "what not to upload" guidance	[Insert]
Over-collection or scope creep	Processing beyond the assessed purpose	Purpose limitation; approved workflow templates; PIA update before new uses	[Insert]
Inaccurate AI output	Incorrect information influencing a decision or communication	Human review checkpoints; cited sources; no autonomous decisions about individuals	[Insert]
Foreign legal reach (residual)	Theoretical access under foreign legal instruments despite Canadian residency	Canadian residency enforcement; CMEK where required; contractual terms; 30/90-day retention	[Insert]
Vendor access during support	Exposure of content to vendor personnel	Contractual confidentiality; audit logging; written authorization before support access	[Insert]

11. Element 9 — Prevention and mitigation

Unauthorized access	enforce named accounts and role-based access; remove accounts promptly; review admin roles quarterly. Owner: [Insert role].
Staff error	orientation on permitted content and DLP behaviour; require review before sending or publishing; issue a one-page "what not to upload" guide. Owner: [Insert role].
Over-collection	limit workflows to approved templates; review new use cases against this PIA before adoption. Owner: [Insert role].
Inaccurate output	require staff review of all AI-assisted outputs; use cited sources; no decisions about individuals without human verification. Owner: [Insert role].
Foreign legal reach	maintain Canadian residency; enable CMEK if required by the risk decision; keep retention short; record the residual-risk decision. Owner: [Insert role].
Vendor access	contractual confidentiality; audit logging; written authorization before support accesses tenant content. Owner: [Insert role].
Privacy breach	follow the municipality's breach-response procedure — contain, assess against RROSH, notify the IPC and affected individuals where required, record the breach, and review causes. Owner: [Insert role].

12. Element 10 — Other prescribed information

At the date of this template, no additional content elements have been prescribed for MFIPPA PIAs beyond those listed above. Record the institution's attestations here:

- ☐ Notice of collection updated to reflect the platform use.
- ☐ Personal information bank (PIB) entry reviewed and updated where required.
- ☐ Records retention schedule reviewed for platform-generated records.
- ☐ Subscription agreement and data-processing terms on file.
- ☐ Staff acceptable-use or AI-use policy communicated.
- ☐ Breach-response procedure current and accessible to staff.

Bill 194 readiness: [ ] tool registered in the AI inventory; [ ] responsible officer named; [ ] public information published; [ ] human oversight assigned; [ ] risk level recorded with a review date.

13. Residual jurisdictional risk and decision

The vendor's cloud provider is headquartered in the United States. While all processing and storage are pinned to Montréal, US legal instruments such as the CLOUD Act can theoretically reach providers headquartered in the United States. Mitigations: enforced Canadian residency, CMEK where enabled, contractual data-processing terms, and short retention cycles (30/90-day purge).

Residual risk accepted / not accepted	[Institution to decide and document].
Overall assessment	[The deployment is approved. / Approved subject to the conditions below. / Not approved at this time.]
Conditions, if any	[Insert — e.g., CMEK required before go-live; health information excluded; annual review.]

14. Sign-off

Assessment completed by	[Name / title / signature / date]
Privacy review	[Name / title / signature / date]
IT / security review	[Name / title / signature / date]
Head of institution or delegate	[Name / title / signature / date]

By signing, the institution records that it has reviewed this assessment, understands the identified risks, and has decided whether to proceed on the terms recorded in Section 13.

Appendix A: Documents reviewed

1. TrueNorth Civic AI — Data Residency & Security Architecture Brief.
2. TrueNorth Civic AI — MFIPPA Compliance Brief.
3. Subscription agreement and data-processing terms.
4. Institution notice of collection and personal information bank entry.
5. Institution records retention schedule.
6. Institution breach-response procedure.
7. Staff AI-use or acceptable-use policy.

This template is provided for information and procurement support. It is not legal advice. The municipality remains the institution responsible under MFIPPA for completing and approving this assessment and for its own notice, retention and breach-response practices.