

Claude Cowork for Ontario municipalities: secure administrative work under MFIPPA

Mike Pearlstein, CISSP, MSc Computer Science (AI)

Published May 27, 2026; Updated August 12, 2026



WHAT'S INSIDE

1. Can Ontario municipalities use Claude Cowork under MFIPPA?
2. What does Claude Cowork actually do for a municipality, explained
3. The MFIPPA and records guardrails
4. What MFIPPA section 30.1 requires of a municipality from January 1, 2027
5. The oversight gap for FOI and records audits
6. Cowork versus the AI already inside your municipal software
7. How much does Claude Cowork cost a municipality?
8. Plan tier and a setup checklist for a municipality
9. Where a municipality should start this week

10. Frequently Asked Questions

fusioncomputing.ca · 416-566-2845 · CISSP-led managed IT, cybersecurity, and AI for Canadian SMBs · Toronto · Hamilton · Metro Vancouver



TRUSTED BY

Toronto law firms Hamilton manufacturers

Vancouver clinics GTA accounting firms Ontario non-profits

British Columbia professional services.

Municipal staff want to know whether Claude Cowork can take on report and document work without breaching MFIPPA or mishandling a record headed for a freedom-of-information request. According to **Statistics Canada** (2026), 19.2% of Canadian businesses used AI in the 12 months to the second quarter of 2026. Public administration sits outside that survey, so municipalities have no benchmark of their own.

Mike Pearlstein, CISSP, MSc Computer Science (AI), founder of Fusion Computing, which has secured IT for Ontario organizations across Toronto, Hamilton, and Metro Vancouver since 2012.

A municipality does not need a different tool than everyone else. It needs the agent pointed at 1 administrative folder, a decision on record about whether sessions run in Anthropic's cloud, and a clerk on anything a resident or the Commissioner will ever read.

Mike Pearlstein, CISSP, founder of Fusion Computing.

Key takeaways.

Book a Consultation

- Claude Team runs from 2 to 150 members at US\$20 per seat per month billed annually, so a clerk and 1 analyst can pilot without a corporate purchase.
- Scope Cowork to 1 administrative folder, never the records or property system.
- Local sessions sit outside your audit trail. Cowork run through web and mobile is captured in the Compliance API, and on Enterprise that cloud mode is off until an owner turns it on.
- Ontario Bill 194 does not cover municipalities. MFIPPA does, and section 30.1 adds breach reporting to the Commissioner from January 1, 2027.
- A clerk or privacy lead reviews anything public-facing. Keep resident information out unless an assessment says otherwise.

Can Ontario municipalities use Claude Cowork under MFIPPA?

Yes, on a Team or Enterprise plan. According to [Anthropic's commercial terms](#) (2026), "Anthropic may not train models on Customer Content from Services". Your MFIPPA duties survive that promise, so scope the agent to a folder holding no personal information and put the rule in writing before staff open it.

The duty to protect personal information is the municipality's, and no vendor setting removes it. What a council controls is the scope: which files the agent opens, which plan governs the data, and whether any resident information is involved at all.

This spoke applies the secure-adoption logic from the pillar guide on [using Claude Cowork securely in your business](#) to a [MFIPPA](#) institution, and it sits alongside our broader [IT for Ontario municipalities](#) work.

Councils that also run grant-funded programs alongside a registered charity will find the same guardrails in our [Claude Cowork guide for non-profits](#).

What does Claude Cowork actually do for a municipality, explained

It finishes multi-step document work. According to [Anthropic’s release notes](#) (2026), Cowork reached general availability on macOS and Windows on April 9, 2026, then gained web and mobile access on July 7, 2026. In a municipal office that means reports, by-laws, notices, grants, and records prep.

Here’s how those 5 jobs map to the work, with the guardrail that keeps each one inside MFIPPA. Fusion Computing walks councils through this before any pilot, the same way we scope any [AI services](#) engagement.

[Book a 30-minute call to scope Claude Cowork for your municipality safely](#)
→

Task	What to test	The guardrail that keeps it safe.
Council reports and agendas	Drafts reports, agendas, and minutes from staff notes	No personal information in the source folder.
Policy and by-law organization	Sorts and updates policies and by-laws	Internal documents, no resident data.
Public notices and communications	Drafts notices and communications	De-identified or already-public content only.
Grant and funding applications	Assembles applications from program materials	Internal program data, reviewed before filing.
Records and FOI-response prep	Organizes records that hold no personal information	Resident data stays out unless assessed.

Treat these as pilot hypotheses to validate in your own tenant, not vendor-guaranteed capabilities. Anthropic documents a subset of them directly; the rest are workflows to test before a firm relies on them.

The MFIPPA and records guardrails

Least privilege is the whole control. According to [Anthropic's safety guidance](#) (2026), prompt-injection risk stays “non-zero” even with classifiers running. The folder you point the agent at is the real boundary, so start with an administrative folder that holds no resident identifiers.

The first thing I check is scope. When a municipality points the agent at a records system, 1 task can touch personal information across every file. Scope it to an administrative folder and you have cut most of the MFIPPA exposure.

FIELD NOTE FROM MIKE. The first thing I draw is a hard line around anything carrying resident information. I've watched a clerk point an agent at a shared drive that also held the property file. We started again with reports, policies, and grant applications, and the workflow that felt reckless became routine.

What may go in, and what must not.

- **In:** draft council reports, by-law text, program materials, and already-public notices.
- **Out:** resident names, addresses, account numbers, and anything in the records or property system.
- **Out:** case files, complaint records, and by-law enforcement material.
- **Always:** a clerk or privacy lead on anything a resident or the Commissioner will read.

Anthropic documents 3 approval modes, and the one a municipality wants is Manually approve. Deletion is protected in every mode, since Cowork “requires your explicit permission before permanently deleting any files”. Treat that as a floor rather than a scoping control.

The policy is the other half. A short rule set names the approved tool, the data that may go in, and who may run it, and I keep it to 1 page for a council. We cover the shape of it in our guide on [what belongs in an AI acceptable use policy](#), paired with a [cybersecurity](#) review so the municipality has a defensible position.

What MFIPPA section 30.1 requires of a municipality from January 1, 2027

Three new duties land together. According to the [Municipal Freedom of Information and Protection of Privacy Act](#) (2026), section 30.1 obliges a head to report qualifying breaches to the Commissioner. The head must also notify the affected resident and keep a record of every reported breach. It was added by 2026, c. 2, Sched. 11, s. 11.

REGULATOR QUOTE. MFIPPA s.30.1(1) says the head “shall report to the Commissioner any theft, loss or unauthorized use or disclosure of personal information in the custody or under the control of the institution”. That duty is triggered where there is a real risk of significant harm. Subsection (8) then requires the head to “keep and maintain a record of every” such reported breach.

The same 2026 amendments add section 28(3), a written privacy impact assessment before collecting personal information. Item 5 of that assessment asks for the position titles of everyone who will have access. An agent pointed at a folder is exactly that access question, arriving 6 months early.

Why Bill 194 is the wrong statute to reach for.

Ontario Bill 194 does not cover municipalities. O. Reg. 51/26 prescribes 5 categories of institution under it: FIPPA educational institutions, Group A, B and C hospitals, the University of Ottawa Heart Institute, children's aid societies, and school boards. A municipality is none of those, and I have watched 2 councils budget for the wrong compliance project because of it.

CONTRARIAN THESIS. Canadian data residency is not a legal requirement, and selling it as one is a myth. PIPEDA Principle 4.1.3 permits transfer outside Canada with comparable contractual protection, and Quebec's Law 25 s.17 asks for an assessment and a written agreement rather than a ban. Choose residency because it makes accountability cheap to evidence, not because a statute forces it.

The oversight gap for FOI and records audits

Where the session runs decides the record. According to **Anthropic's admin guidance** (2026), local session history stays on the user's computer and "cannot be centrally managed or exported by admins". Cowork via mobile and web is captured in the Compliance API instead.

That split is the setting I check first on any municipal engagement. Cloud sessions are on by default for Team plans and off by default for Enterprise, where an owner switches them on and grants the capability through custom roles.

Where the record actually lives.

- **Local session:** history sits on the laptop, outside admin export and outside the Compliance API.
- **Web or mobile session:** runs on Anthropic infrastructure and is captured in the Compliance API.

- **OpenTelemetry stream:** tool calls and file access, in your own monitoring, for either mode.

The Enterprise **audit logs** capture metadata rather than the work itself. Owners can also stream Cowork events to a SIEM through OpenTelemetry, which Anthropic notes “doesn’t replace audit logging for compliance purposes” on its own. Cowork exports the full text of user prompts by default, along with tool parameters, file paths and user email addresses, so configure filtering or redaction at the collector and set SIEM access and retention before enabling export. Our engineers found that stream is where tool calls and file access become visible.

If the pilot needs centralized monitoring, define the destination, filtering, access and retention before enabling OpenTelemetry.

Cowork versus the AI already inside your municipal software

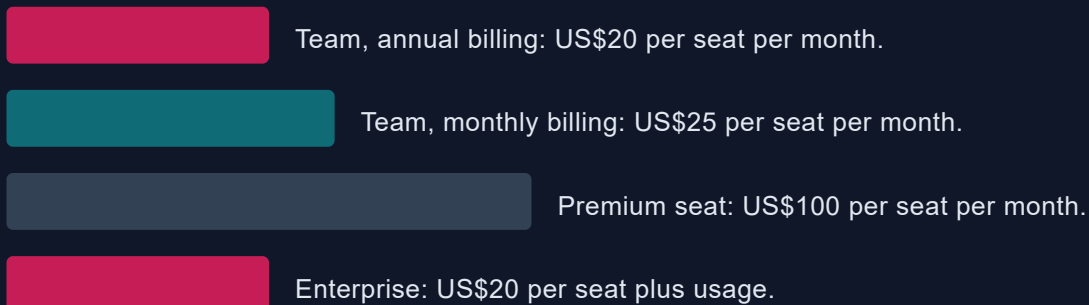
Blast radius is the difference. Municipal AI is embedded in an agenda, records, or tax system and is scoped to that system’s data. Claude Cowork reaches across your own files instead, so an agenda module sees 1 dataset while a desktop agent sees whatever folder and connectors an owner granted it 5 minutes ago.

That difference cuts both ways, and the question I ask first is which system already hands you an audit trail. An agenda-management vendor usually carries part of that burden for you. With Cowork the municipality owns the scoping decision, so the upside is that the agent works on the odd, cross-system documents no platform ever covered.

How much does Claude Cowork cost a municipality?

Less than the scoping work around it. According to Anthropic's published pricing (2026), Claude Team is built for 2 to 150 members at US\$20 per seat per month billed annually, or US\$25 billed monthly. A premium seat with 5 times the usage is US\$100. Enterprise is US\$20 per seat plus usage at API rates.

Claude plan pricing, 2026 (US dollars).



Team	Team, annual billing: US\$20 per seat per month.
Team	Team, monthly billing: US\$25 per seat per month.
Premium seat	Premium seat: US\$100 per seat per month.
Enterprise	Enterprise: US\$20 per seat plus usage.

Two numbers matter when I size this for a council. The floor is 2 licences, so a clerk and 1 analyst can pilot without a corporate purchase. The ceiling is 150 people, above which the plan is Enterprise.

In our practice the licence is rarely the expensive part. We measured the real cost sitting in scoping, policy drafting, and the monitoring wiring, at 3 to 6 hours for a small Ontario municipality rather than a per-seat charge.

Charities and non-profit partners a municipality funds may qualify separately: Anthropic announced Claude for Nonprofits on December 2, 2025, with up to 75% off Team and Enterprise. Anthropic publishes no eligibility test naming municipalities either way, so put the question to your account team rather than assuming.

Plan tier and a setup checklist for a municipality

Plan tier is the first decision. According to [Anthropic's privacy centre](#) (2026), an individual plan with the improvement setting enabled may keep chats “in a de-identified format for up to 5 years in our model training pipelines”. Business inputs and outputs are deleted within 30 days by default.

Need the policy first? Use our [AI acceptable use policy template](#).

That 5-year gap is the whole argument for buying 2 seats, because only Team and Enterprise carry the contractual no-training commitment plus the admin controls a council needs.

Why Canadian organizations bring this work to Fusion Computing.

CISSP-led, a Microsoft Solutions Partner and a CompTIA Managed Services Trustmark holder, securing IT for Canadian SMBs across Toronto, Hamilton, and Metro Vancouver since 2012.

[Get a CISSP-led review of where AI tools touch resident information →](#)

The 8-step rollout.

1. **Choose Team or Enterprise.** Staff running municipal work on a personal account is the first risk to fix.
2. **Scope to 1 administrative folder.** Never the records or property system. Widen only with a reason.
3. **Set the approval mode to Manually approve.** Deletion always prompts, and resident data should too.
4. **Decide the cloud-session question.** Team has it on by default; Enterprise owners must switch it on deliberately.
5. **Write an acceptable use policy.** Name the approved tool, the data that may go in, and who may run it.

6. **Turn on OpenTelemetry monitoring only after deciding what may be logged.** On local sessions it's an additional visibility stream into what the agent did.
7. **Keep the clerk or a privacy lead signing off.** Nothing public-facing ships without review.
8. **Start the section 28(3) assessment now.** The written privacy impact assessment duty begins January 1, 2027.

FIELD NOTE FROM MIKE. I ask 1 question before any of the 8 steps above: who reviews this document today, when a human writes it? If nobody at the municipality can name that person, the AI pilot is not the problem I want to solve first. Cowork simply makes an informal review step visible sooner than the Commissioner would.

None of it's exotic. The technical setup can be quick; the privacy, logging and approval work is what decides how long the pilot takes. Fusion Computing sets it up as part of the **managed IT** work we already do for public-sector clients across **Toronto and the GTA**. The same pattern carries to **law firms** and **architecture and engineering firms** under their own rules.

Where a municipality should start this week

Buy 2 Team seats and scope them to 1 administrative folder. Keep resident information out of it, set approvals to Manually approve, and put the cloud-session decision in writing before anyone opens a second folder. Fusion Computing runs that scoping session in an afternoon. If you want a CISSP-led second opinion first, **talk to us** or read more **about how we work**.

Frequently Asked Questions

Q. Can a municipality put resident information into Claude Cowork?

Treat that as a decision, never a default. Personal information sent to Cowork reaches Anthropic, so it leaves the municipality's direct control. Keep resident information out of the tool, de-identify data before processing, or complete a written assessment first. Administrative work with no personal identifiers is the safe starting point, and from January 1, 2027 MFIPPA s.28(3) makes that written assessment a statutory duty before collection.

Q. Is Claude Cowork MFIPPA-compliant?

MFIPPA compliance depends on how a municipality uses a tool, never on the tool alone. Cowork can be used in an MFIPPA-aligned way for administrative tasks with no personal information, on a business plan, with a policy and a privacy lead involved. Anthropic's commercial terms say it may not train models on Customer Content, and business inputs and outputs are deleted within 30 days by default.

Q. Does Ontario Bill 194 apply to municipalities?

No. O. Reg. 51/26 prescribes 5 categories of institution under Bill 194: FIPPA educational institutions, Group A, B and C hospitals, the University of Ottawa Heart Institute, children's aid societies, and school boards. Municipalities are not among them. The instrument that governs a municipality is MFIPPA, and the 2026 amendments in c. 2, Sched. 11 add breach reporting, resident notification, and a breach record from January 1, 2027.

Q. What plan does a municipality need for Claude Cowork?

—

Team or Enterprise, never a personal Pro or Max account. Claude Team runs from 2 to 150 members at US\$20 per seat per month billed annually. Above that ceiling, or where you need groups and custom roles to enable Cowork for 1 department only, the answer is Enterprise. Staff running municipal work on a consumer account is the first risk to remediate, and it is the first thing our CISSP-led review looks for.

Want an MFIPPA-aware AI use policy before staff pilot Cowork? →

Q. Does the Compliance API capture what staff do in Cowork?

—

It depends on where the session runs. Local session history stays on the user's computer and cannot be centrally managed or exported by admins. Cowork via mobile and web is captured in the Compliance API, and a Compliance Access Key with the right scope can read those remote sessions and their transcripts. Anthropic enables the Compliance API self-service for Claude Enterprise organizations and on request elsewhere.

Q. Is our data used to train the model?

—

On Team and Enterprise plans, Anthropic's commercial terms say it may not train models on Customer Content from the Services. A personal Pro or Max account is different: with the improvement setting enabled, chats may be kept in de-identified form for up to 5 years in Anthropic's training pipelines. For a municipality, that 5-year gap is the reason to standardise on business seats.

Q. Does Claude Cowork work on Windows or only Mac?

Both, and on more surfaces since launch. Cowork reached general availability on macOS and Windows through the Claude desktop app on April 9, 2026. On July 7, 2026 Anthropic added web at claude.ai and the Claude mobile apps, in beta for Team and Enterprise, with those sessions running on Anthropic's infrastructure rather than the laptop. Confirm the current feature list inside the app.

Q. Who at the municipality should run Claude Cowork?

Start with administrative staff and a privacy lead, never the whole organization and never staff handling resident records. The Cowork toggle is organization-wide, so a Team plan is all-or-nothing. On Enterprise, groups and custom roles let an admin enable Cowork, or the cloud-session capability, for named teams only. Pair whichever you choose with training and a written policy, which is the CISSP-led review Mike Pearlstein runs before a pilot.

Talk to Fusion

Put this guide to work

Fusion Computing helps Canadian SMBs adopt AI safely. The review work is CISSP-led at a Microsoft Solutions Partner and CompTIA Managed Services Trustmark holder, securing Canadian businesses since 2012.

- Managed IT support with a 1-hour priority response
- Cybersecurity, managed detection and response, and compliance reviews
- AI and Copilot consulting, including safe Claude Cowork pilots
- Microsoft 365 management and licensing

Book a 30-minute scoping call

fusioncomputing.ca/contact-us · 416-566-2845
Toronto · Hamilton · Metro Vancouver