

# AI Adoption in BC Municipalities

FOIPPA, data sovereignty,  
and Microsoft 365 Copilot



A WHITE PAPER BY ALPHA IT

VERSION 1.0 · APRIL 2026

## AUTHOR'S NOTE

This paper was prepared by ALPHA IT to support BC municipal leaders evaluating governed AI adoption under FOIPPA. Key legal and vendor statements are sourced.

This paper is for informational purposes only and is not legal advice. Municipalities should consult their privacy and legal counsel and complete appropriate Privacy Impact Assessments (PIAs) for any initiative involving personal information.



## EXECUTIVE SUMMARY

## The risk-based reality of municipal AI in BC

British Columbia municipalities are under growing pressure to modernize service delivery while strengthening data protection and public accountability. Artificial intelligence — particularly generative AI — offers clear productivity and service benefits, but also introduces legitimate concerns around privacy, data sovereignty, and foreign access to information.

This paper outlines three realities municipal leaders must address:

- ▲ **The risk environment has changed.** Geopolitical instability, nation-state cyber activity, and increasingly sophisticated attacks mean public-sector data protection is now a governance-level responsibility — not just an IT issue.
- ▲ **Data residency is not the same as data sovereignty.** Even when data is stored in Canada, U.S.-headquartered cloud providers may be subject to foreign legal access under laws such as the U.S. CLOUD Act.<sup>[3][4]</sup>
- ▲ **Microsoft 365 Copilot — including Anthropic's Claude models — represents a measured and defensible approach** when deployed with proper governance, Privacy Impact Assessments (PIAs), and controls.<sup>[1]</sup>

There is no “zero-risk” option. The objective for municipalities is to understand risks clearly, document decisions transparently, and adopt AI tools in a way that aligns with FOIPPA, public trust, and operational realities.



## SECTION 01

## The global risk context

Municipal governments now operate in one of the most hostile digital environments in history. Cyber threats increasingly involve organized groups and nation-state actors targeting public infrastructure and essential services. Local governments hold information that is operationally critical and politically sensitive — public safety records, social services data, land and infrastructure information, and employee records.

Avoiding modern tools altogether is not a viable response. Prohibiting AI often leads to ungoverned “shadow AI” use by staff, which increases risk rather than reducing it. The challenge is to adopt AI deliberately, within a controlled and auditable framework.<sup>[5]</sup>

## SECTION 02

## FOIPPA and the shift to risk-based decision making

BC municipalities are governed by the Freedom of Information and Protection of Privacy Act (FOIPPA) (RSBC 1996, c. 165).<sup>[1]</sup> In 2021, Bill 22 removed the long-standing prohibition on storing personal information outside Canada.<sup>[2]</sup> It was replaced with a risk-based framework: municipalities may now use cloud or AI services that involve out-of-Canada storage or access, provided they conduct a PIA under section 33.1, identify applicable foreign laws, document safeguards, and make an informed, documented decision.<sup>[1][11]</sup>

## SECTION 03

## Data residency vs. data sovereignty

A persistent misconception is that “data stored in Canada cannot be accessed by foreign governments.” This is not correct.

### DATA RESIDENCY

Refers to **where data is physically stored**. Canadian hosting can reduce some operational and latency risks — and satisfies many procurement questions — but it is a geographic fact, not a legal shield.

### DATA SOVEREIGNTY

Refers to **which laws can be applied to that data**. A U.S.-parented provider may be compelled to disclose records under U.S. law even when the data never leaves Canada.

Under the U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act, enacted March 2018), U.S.-headquartered companies can be compelled to provide data under their control *regardless of where it is stored*. The Act specifies that service providers must comply with lawful demands to disclose stored data in their “possession, custody, or control, regardless of the location of the data.”<sup>[3][4]</sup>

In 2025, Microsoft executives confirmed under oath before the French Senate that they cannot guarantee data stored outside the U.S. would never be disclosed to U.S. authorities if legally compelled.<sup>[7][8]</sup>

### THE IMPLICATION FOR BC MUNICIPALITIES

Canadian data centres reduce risk, but do not eliminate foreign legal exposure when using U.S.-based hyperscale providers. FOIPPA’s current framework reflects this reality — it does not assume perfect sovereignty; it requires municipalities to understand and manage residual risk.



## SECTION 04

## Why Microsoft is commonly chosen in the public sector

Despite jurisdictional complexity, Microsoft is widely used across Canadian public-sector organizations, including in British Columbia. This reflects a pragmatic risk-benefit assessment.

- ▲ **Canadian data centres and investment.** Microsoft operates major data centre regions in Canada Central (Toronto) and Canada East (Quebec City) and has committed billions in additional Canadian cloud and AI infrastructure investment.<sup>[9][10]</sup> Core Microsoft 365 workloads — email, files, collaboration — can be hosted at rest in Canada.
- ▲ **Security at scale.** Microsoft invests heavily in cybersecurity, operating global threat-intelligence capabilities and 24/7 monitoring. For many municipalities, this level of security investment exceeds what could realistically be achieved on-premises.
- ▲ **Compliance and governance tooling.** Data classification, retention, audit logging, eDiscovery, and loss-prevention tools support FOIPPA obligations when properly configured.<sup>[5]</sup>
- ▲ **Contractual protections.** Microsoft's enterprise agreements include data-use restrictions, confidentiality obligations, breach notification commitments, and explicit assurances that customer data is not used to train public AI models.<sup>[5][6]</sup>

**The trade-off:** Microsoft does not eliminate cross-border legal risk. It reduces and manages risk through infrastructure, contracts, and transparency. FOIPPA requires municipalities to document this trade-off — not deny it.

## SECTION 05

## Anthropic models within Microsoft 365 Copilot

Anthropic's Claude models are available within Microsoft 365 Copilot as Microsoft-managed services. Anthropic operates as a subprocessor under Microsoft's enterprise data protection framework.<sup>[6]</sup>

- ▲ Prompts and responses are not used to train AI models.<sup>[5]</sup>
- ▲ Data flows remain within Microsoft's tenant and compliance boundary.
- ▲ Administrative controls allow municipalities to enable or disable Anthropic models.
- ▲ Audit and governance tools (via Microsoft Purview) apply.

**Safety and alignment.** Anthropic is known for its Constitutional AI approach, which explicitly prioritizes safety, harm reduction, and alignment with human values. The company published a comprehensive constitution for Claude in January 2026 that details its commitment to making Claude “broadly safe,” “broadly ethical,” “compliant with guidelines,” and “genuinely helpful.”<sup>[12]</sup> For public-sector use, this conservative design philosophy is a meaningful factor — it reduces the likelihood of problematic or inappropriate outputs.

**Data residency considerations.** Anthropic models are currently excluded from in-country processing guarantees.<sup>[5][6]</sup> This means AI inference may occur outside Canada, typically in the United States. From a FOIPPA perspective, this is not a prohibition — but it requires explicit acknowledgement in the PIA, careful consideration of data sensitivity, and appropriate usage policies and safeguards.



## SECTION 06

## Why this is preferable to unmanaged AI use

The relevant comparison is not “Copilot vs. zero risk.” It is **governed, enterprise AI vs. unmanaged consumer tools**. Without sanctioned tools, staff often use public AI services on their own — which may retain prompts for model training, lack audit logs or administrative oversight, and operate outside municipal contracts or policies.

## SECTION 07

## Remaining risks and how to manage them

There is no zero-risk configuration. Responsible AI adoption requires acknowledging residual risks and managing them deliberately.

### KEY RISKS

- Foreign legal access under U.S. law (CLOUD Act, 18 U.S.C. § 2713).<sup>[3][4]</sup>
- AI processing outside Canada for certain models.<sup>[5][6]</sup>
- Configuration errors under the shared responsibility model.
- Human misuse or over-reliance on AI outputs.
- Evolving threat and regulatory landscapes.

### PRACTICAL MITIGATIONS

- Complete robust PIAs documenting data types, sensitivity, foreign access risks, and mitigations under FOIPPA s. 33.1.<sup>[1]</sup>
- Implement layered controls — data classification, DLP, audit logging, and access governance.
- Define clear usage policies specifying permitted use cases and prohibited data.
- Train staff to treat AI as assistive — not an authority.
- Review and reassess regularly as vendor capabilities and regulations evolve.
- Be transparent: clear internal and external communication builds trust.



## SECTION 08

## What municipal leaders should do next

---

If you are evaluating AI in your organization, start here:

- ▲ Identify where AI is already being used, including unsanctioned tools.
- ▲ Understand what data is being shared and where risk may exist.
- ▲ Define a small set of acceptable use cases and develop simple guardrails.
- ▲ Complete a Privacy Impact Assessment before expanding usage.
- ▲ Assign clear accountability for oversight.

## SECTION 09 · CONCLUSION

## ALPHA IT's perspective

---

Microsoft 365 Copilot, including Anthropic's models, does not eliminate sovereignty or security concerns. It does, however, provide a controlled, auditable, and enterprise-grade environment that aligns with FOIPPA's risk-based framework when deployed responsibly. With clear governance, transparent decision-making, and trusted partners, municipalities can adopt AI in a way that improves service delivery while respecting privacy, legislation, and public trust.

**THE ALPHA IT APPROACH**

ALPHA IT is a BC-based consultancy focused on helping municipalities adopt technology pragmatically and defensibly. Our approach is grounded in *honesty about risk*, *alignment with BC law and accountability*, and *practical governance*. We help municipalities complete FOIPPA-aligned PIAs, configure Microsoft 365 and Copilot securely, develop AI governance and acceptable-use frameworks, and make decisions that stand up to public, regulatory, and council scrutiny.



## REFERENCES

## Sources &amp; further reading

- [1] **Freedom of Information and Protection of Privacy Act**, RSBC 1996, c. 165 — Government of British Columbia, *Section 33.1 — Disclosure Outside of Canada*, FOIPPA Policy & Procedures Manual.  
bclaws.gov.bc.ca/.../96165\_00
- [2] **Freedom of Information and Protection of Privacy Amendment Act, 2021** (Bill 22). Government of British Columbia.  
bclaws.gov.bc.ca
- [3] **Daskal, J., & Salgado, R. (2025)**. CLOUD Act: Answers to Frequently Asked Questions. Cross Border Data Forum.  
crossborderdataforum.org
- [4] **U.S. Department of Justice (2018)**. CLOUD Act Resources — 18 U.S.C. § 2713.  
justice.gov/criminal/cloud-act-resources
- [5] **Microsoft Learn (2024)**. Data, Privacy, and Security for Microsoft 365 Copilot.  
learn.microsoft.com/.../microsoft-365-copilot-privacy
- [6] **Microsoft Learn (2026)**. Anthropic as a subprocessor for Microsoft Online Services.  
learn.microsoft.com/.../connect-to-ai-subprocessor
- [7] **Woollacott, E. (Forbes, Jul 22, 2025)**. Microsoft Can't Keep EU Data Safe From US Authorities.  
forbes.com/.../microsoft-cant-keep-eu-data-safe-from-us-authorities
- [8] **The Register (Jul 25, 2025)**. Microsoft exec admits it 'cannot guarantee' data sovereignty.  
theregister.com
- [9] **Microsoft (2025)**. Microsoft to spend \$7.5B on AI data centre expansion with pledge to protect Canada's digital sovereignty. *BetaKit*.  
betakit.com
- [10] **Microsoft (2026)**. Ontario Welcomes Microsoft's AI Infrastructure Expansion. Ontario Newsroom.  
news.ontario.ca
- [11] **McCarthy Tétrault (2021)**. British Columbia Unveils Significant Changes to FIPPA Including New Data Sovereignty Rules.  
mccarthy.ca
- [12] **Anthropic (2026)**. Claude's new constitution.  
anthropic.com/news/claude-new-constitution

## NANAIMO, BC

304-321 Wallace Street  
Nanaimo, BC V9R 5B6  
+1 778 441 2535

## COURTENAY, BC

3-2760 Cliff Avenue  
Courtenay, BC V9N 2L6  
+1 778 441 2535

## GET IN TOUCH

info@getalpha.ca  
[getalpha.ca](https://www.getalpha.ca)  
AI + IT Services