

Counsel Review Checklist: AI Acceptable Use Policy (Canada)

The Canadian legal questions to put to your lawyer or privacy professional before adopting an AI use policy.
Companion to the AI Acceptable Use Policy Template for Canadian Organizations, v1.2.

Version 1.2 | Published July 2026, updated October 2026 | Prepared by Mandate Systems Inc. | Next review: July 2027

Not legal advice. This checklist is general information, not legal advice, and reading or using it creates no lawyer-client relationship. It was prepared by a vendor, Mandate Systems Inc., not by your counsel.

The questions, by statute

This checklist deliberately asks rather than asserts. Statutory duties depend on your province, sector, and clients; your counsel answers these, and their answers shape the policy.

- ☐ **PIPEDA (federal private sector).** Does PIPEDA govern our handling of personal information, in whole or in part? Do our identified purposes and consents cover entering personal information into the AI tools we have approved? What do we owe when a tool's provider processes data outside Canada?
- ☐ **Quebec, Law 25.** Do we serve Quebec individuals or operate in Quebec? If so: do any of our AI uses amount to a decision based exclusively on automated processing, triggering the transparency duty? Does entering personal information into a tool hosted outside Quebec require a privacy impact assessment for communication outside the province? Are our consent practices sufficient under Law 25's standards?
- ☐ **Quebec, French language.** If we have staff in Quebec: does the Charter of the French language require this policy, the training in section 11, and the acknowledgment in Appendix E to be available in French?
- ☐ **Provincial private-sector and health statutes.** Do PIPA (British Columbia), PIPA (Alberta), PHIPA (Ontario), or HIA (Alberta) apply to any information we hold? If we are a health information custodian or an agent of one, which of this policy's rules need to be tightened to match custodian duties?
- ☐ **Retention and deletion.** When an engagement ends or a tool leaves our register, what do our retention and destruction obligations require for information already inside AI tools, and do the tools we have approved let us meet them?
- ☐ **Ontario employment law.** Do we have enough Ontario employees to require a written electronic monitoring policy, and does section 8.3 of this policy satisfy that requirement as written?
- ☐ **Professional obligations.** What do our regulator's rules and guidance on confidentiality and technology use require of us specifically? (Your regulator's confidentiality rules and any guidance it has issued on generative AI.)
- ☐ **Regulated-sector overlays.** If we handle work subject to FINTRAC, OSFI, or CRA obligations, or to a securities regulator: do any of those regimes constrain the tools or data flows this policy would otherwise permit?
- ☐ **Insurance.** Our cyber insurer may ask whether we have a written AI use policy and how it is enforced. Does anything in our current coverage turn on the answers?

Reuse. You may copy, adapt, and use this checklist inside your organization without permission, payment, or attribution. If you republish it publicly, credit Mandate Systems Inc. and link to mandateco.ca.

About the preparer. Mandate Systems Inc. (mandateco.ca) is a Canadian company that builds the enforcement and record layer behind policies like this one. The checklist stands on its own; nothing in it requires our product.