

AI Acceptable Use Policy Template for Canadian Organizations

A PIPEDA and Law 25 aware template. Free to adapt with your counsel.

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

Before you adopt this. This template 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. Privacy and professional obligations differ by province, sector, and client base, and a policy only helps if it matches yours. Have a lawyer or privacy professional adapt it before adoption, then delete this notice. One limitation to keep in view: a policy sets obligations, and on its own it does not enforce anything or leave a record. Appendix B lists the records that would show this policy is being followed.

How to use this template

Guidance: this section is for the person adapting the template. Delete the whole section, and every block that begins with "Guidance:", before adoption.

1. Assign an owner. One named role holds this policy (section 3). Pick it first; every other decision has a home once someone owns the document.
2. Fill the placeholders. Everything in [square brackets] needs a real value: your organization's name, named roles, contact points, and dates.
3. Pick any optional clauses. Appendix D has optional clauses for privileged legal material, client financial records, and personal health information. Paste the ones that apply into section 5, or skip them.
4. Have counsel review it. Appendix C lists the Canadian legal questions to put to your lawyer or privacy professional, by statute. This template deliberately asks those questions rather than answering them.
5. Roll it out with acknowledgment. Section 11 and Appendix E cover training and signed acknowledgment.

A note on the "Evidence expectation" lines: each section of this policy ends with one line naming the record that would show the section is being followed. Every one of them can be kept by hand: a register, a signed form, a dated note. Appendix B collects them into a single checklist you can hand to an auditor, an insurer, or your own board.

1. Purpose and scope

- 1.1 This policy sets the rules for using artificial intelligence tools in the work of [Organization].
- 1.2 It applies to every employee, contractor, student, and volunteer who handles [Organization] information or systems ("staff" in this policy).
- 1.3 It covers three kinds of AI use, on any device used for [Organization] work:
 - (a) standalone AI tools, such as chat assistants used through a website or app;
 - (b) AI features inside software [Organization] already licenses, such as drafting assistants, meeting summarizers, and coding assistants;
 - (c) AI agents: software that takes actions with real effect, such as sending messages, filing documents, running code, or completing transactions.
- 1.4 The policy applies whether the tool is free or paid, and whether or not IT installed it.

2. Definitions

AI system. Software that generates content, predictions, recommendations, or decisions from a model trained on data. This includes generative AI (tools that produce text, images, audio, or code).

AI agent. An AI system that can take actions with real effect, such as sending an email, modifying a file, calling another system, or making a commitment, rather than only producing output for a person to review.

Approved AI tool. An AI system listed in the tool register (Appendix A) with a current approval date.

Personal information. Information about an identifiable individual, as defined by the privacy law that applies to [Organization].

Confidential information. Information [Organization] is obliged to protect: client and customer information, employee records, financial records, and anything covered by a contract, undertaking, or professional duty of confidentiality.

3. Roles and responsibilities

3.1 [Policy Owner, e.g. Privacy Officer or CISO] owns this policy, maintains the tool register (Appendix A), decides exceptions (section 10), and reports on the policy's operation to [governing body, e.g. the board] at least annually.

3.2 [Approver role, e.g. IT lead or Privacy Officer] evaluates and approves tools before they enter the register, and records the basis for each approval.

3.3 [IT contact] configures approved tools, manages accounts, and disables access when someone leaves.

3.4 Every staff member must use AI tools within this policy, complete the training in section 11, and report incidents under section 9.

Evidence expectation: the current signed policy with a named owner and approval date, and the most recent report to [governing body].

4. Approved and prohibited tools

4.1 Staff must use only approved AI tools (Appendix A) for [Organization] work. The one exception is the public-information allowance in 4.2.

4.2 Work data must go only through [Organization]-controlled accounts on those tools. Personal accounts have one permitted use: information that is already public and contains nothing from section 5.2 or 5.3. When in doubt, treat it as work data.

4.3 A tool is approved for the uses and data classes recorded in the register, not for everything. The register states what each tool may touch.

4.4 Staff must not enter [Organization] information into an unlisted tool to "try it out". Trials go through the exception process in section 10.

4.5 Staff may propose a tool for approval at any time by telling [Approver role] what the tool is and what they want it for. Proposing a tool is always better than improvising with one. Purchases and renewals of software with AI features go through the same door before signing.

4.6 The register also records tools [Organization] has considered and prohibited, with the reason. A prohibited entry overrides every other permission in this policy.

4.7 When a tool leaves the register, [IT contact] closes [Organization] accounts on it, requests deletion of stored [Organization] data where the provider supports it, and records both in the register.

Evidence expectation: a dated tool register showing each tool, its status, its approved uses, its account type, and its last review date.

5. Data rules

Guidance: this is the section staff will actually remember. Keep the table short and blunt. We drafted the classes below as examples; adjust them to the information your organization holds, and paste in any Appendix D clauses that apply.

5.1 The rules below apply per class of information, in any AI tool, in any direction: prompts, uploads, connected data sources, and agent access all count as "entering" information.

5.2 Never enter, in any tool:

- (a) passwords, access keys, API keys, or any other credential;
- (b) information subject to a court order, sealing order, or active litigation hold, unless counsel approves in writing;
- (c) information a contract or undertaking forbids sharing with any third party.

5.3 Only in approved tools cleared for that class, and only the minimum needed for the task:

- (a) personal information of clients, customers, employees, or anyone else;
- (b) client or customer confidential information, including the fact that someone is a client where that fact is itself sensitive;
- (c) financial records of [Organization] or its clients;
- (d) source code, system configurations, and proprietary methods;
- (e) health information;
- (f) material covered by professional privilege or a professional duty of confidentiality.

5.4 **Generally permitted in approved tools:** public information, published material, and drafts that contain none of the classes above.

5.5 Where an approved tool offers a setting to exclude entered data from model training, [IT contact] must enable it, and record in the register where it is not available.

Evidence expectation: dated spot-check notes (or tool logs, where a control exists) showing the rules are checked in practice, not just published.

6. Use of AI outputs

6.1 A person is accountable for every AI output used in [Organization] work. "The AI wrote it" transfers nothing.

6.2 Before AI-assisted work product leaves [Organization], the responsible staff member must verify its facts, citations, calculations, and any statement of law or regulation, and must correct AI errors as their own.

6.3 Staff must not present AI output as the work of a named professional where a client, court, tribunal, or regulator requires disclosure of how the work was produced. When in doubt, ask [Policy Owner].

6.4 Generated content may carry intellectual property risk (training-data provenance, third-party rights). Material intended for publication or commercial use needs review under [Organization]'s existing IP process.

Evidence expectation: the verification step recorded in the matter, engagement, or project file for AI-assisted deliverables.

7. AI agents and automated actions

Guidance: if nobody at your organization uses agents yet, keep this section anyway. It is easier to have the rule before the first agent than after.

7.1 An AI agent must not act on client matters, move funds, sign or commit [Organization] to anything, or send external communications unless a named person has authorized that category of action in advance and is accountable for it.

7.2 Every agent in use must appear in the tool register with: the systems it can reach, the categories of action it may take, and the named person accountable for it.

7.3 Agent access must be scoped to what the task needs. An agent must not run under a person's full account access where narrower access is available.

7.4 Staff must be able to stop an agent they are accountable for, and must know how before first use.

Evidence expectation: register entries listing each agent's permitted action categories and accountable person.

8. Privacy obligations and workforce notice

8.1 Personal information entered into an AI tool is still a use of personal information. It must stay within the purposes [Organization] identified when the information was collected, and within any consent that applies.

8.2 Before adopting a tool that will routinely process personal information, [Policy Owner] must complete a privacy review appropriate to [Organization]'s obligations (Appendix C lists the questions for counsel, including Quebec's Law 25 requirements where they apply).

8.3 **Workforce notice.** [Organization] logs and may review AI use on its systems to enforce this policy. This monitoring is described here so that it is not hidden. Questions about what is logged go to [Policy Owner].

8.4 Where [Organization] has employees in Ontario, counsel should confirm whether the written electronic monitoring policy requirement applies and whether 8.3 satisfies it (Appendix C).

Evidence expectation: dated staff acknowledgments (Appendix E) covering the notice in 8.3.

9. Incident reporting

9.1 Staff must report to [incident contact], without deleting anything, when:

- (a) information from section 5.2 went into any tool, or information from section 5.3 went into a tool not approved for it;
- (b) a credential may have been exposed to an AI tool;
- (c) AI-assisted work product went out with a material error;
- (d) an AI agent took an action outside its authorized categories.

9.2 Reporting an honest mistake promptly is treated as compliance with this policy, not a breach of it.

9.3 Incidents involving personal information go into [Organization]'s existing privacy-breach process, which decides whether notification duties arise.

Evidence expectation: an incident log, dated, even when it records nothing.

10. Exceptions

10.1 Exceptions to this policy require a written request to [Approver role], stating the tool, the data classes involved, the purpose, and the duration.

10.2 Exceptions must be time-bound, and every exception must be recorded in the exception log with its expiry date.

Evidence expectation: the exception log.

11. Training and acknowledgment

11.1 Staff must complete AI-use training at onboarding and annually after that. Training covers this policy, the data rules in section 5, and how to report an incident.

11.2 Each staff member must sign the acknowledgment in Appendix E at onboarding and at each annual renewal.

Evidence expectation: signed acknowledgment forms on file for all current staff.

12. Enforcement

12.1 Breaches of this policy are handled under [Organization]'s existing employment and contractor discipline processes. This policy creates no separate discipline scheme.

13. Review

13.1 [Policy Owner] reviews this policy at least annually, and additionally when: a new tool class comes into use, an incident under section 9 exposes a gap, a pattern in the exception log suggests the policy no longer matches real work, or an applicable law changes.

13.2 Each revision gets a new version number and date in the table below.

Version	Date	Summary of change	Approved by
1.0	[Effective date]	Initial adoption	[Policy Owner]

Evidence expectation: the version table above, kept current.

Appendix A: Tool register

Guidance: one row per tool or agent, including tools you have prohibited (mark the status and record why). The register is referenced by sections 4, 5, and 7. Keep it wherever your other operational registers live; the policy only requires that it exists, is dated, and is reviewed.

Tool / agent	Approved uses	Data classes permitted (per 5.2 to 5.4)	Account type	Training-data exclusion on?	Accountable person	Status, date	Last reviewed
[Tool name]	[e.g. drafting, research]	[e.g. public and internal drafts only]	[Organization] enterprise	[yes / not available]	[name]	[approved, date]	[date]

Appendix B: Evidence checklist

Guidance: this is the one-page view for an audit, an insurance questionnaire, or a board question. Each line repeats an "Evidence expectation" from the policy body.

#	Record	Policy section	Where it lives	Last checked
1	Signed current policy, named owner, latest report to [governing body]	3		
2	Dated tool register	4		
3	Spot-check notes or tool logs for the data rules	5		
4	Verification steps recorded in matter or project files	6		
5	Agent register entries with action categories and accountable person	7		
6	Staff acknowledgments covering the monitoring notice	8		
7	Incident log (dated, even if empty)	9		
8	Exception log with expiry dates	10		
9	Training and acknowledgment records for all current staff	11		
10	Version history table, current	13		

Appendix C: Canadian legal context, as questions for your counsel

Guidance: this appendix deliberately asks rather than asserts. Statutory duties depend on your province, sector, and clients; your counsel answers these, and their answers may change the policy body.

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?

Appendix D: Optional clauses for information with its own duties

Guidance: paste the clauses that apply into section 5, renumber, and delete the others.

D.1 Privileged legal material. Privileged material and anything subject to solicitor-client confidentiality must not enter any AI tool unless the register records that counsel has approved that tool for privileged material, naming the basis. The duty of confidentiality covers the existence of a retainer, not only its contents. Where a court, tribunal, or law society requires disclosure of AI use in a filing or proceeding, the responsible lawyer must comply and must keep the disclosure with the matter file.

D.2 Client financial records. Client financial records, working papers, and anything received under a client agreement must not enter any AI tool unless the register approves that tool for client financial data. Confidentiality duties under your professional code continue to apply in full when a tool is between you and the client's information. Material connected to assurance work needs particular care: treat independence and confidentiality questions as counsel-and-regulator questions, not tool-configuration questions.

D.3 Personal health information. Personal health information must not enter any AI tool unless the register approves that tool for it and the privacy review in 8.2 has been completed for that use. Custodian duties (and agent duties owed to a custodian) apply to AI tools exactly as to any other information system, including limits on use, disclosure, and retention.

Appendix E: Acknowledgment

I confirm that I have read the AI Acceptable Use Policy of [Organization], version [], that I understand the data rules in section 5 and the monitoring notice in section 8.3, and that I know how to report an incident under section 9.

Name: _____ Role: _____

Signature: _____ Date: _____

Reuse, credit, and further reading

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

Further reading (names only; none of these are claims about this template): the Office of the Privacy Commissioner of Canada's PIPEDA guidance; NIST AI Risk Management Framework; ISO/IEC 42001.

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 template stands on its own; nothing in it requires our product.